Soundview Security
info@soundviewsecurity.com

Scan Report

Tue, 16 Apr 2024 17:01:54 West Asia Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

x.x.1.26

10	4	10	0	22
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Tue Apr 16 16:29:55 2024

End time: Tue Apr 16 16:45:31 2024

Host Information

IP: x.x.1.26

OS: Dell EMC VMX, Microsoft Windows Embedded Standard 7

Vulnerabilities

55814 - Adobe Media Server Unsupported Version Detection -

Synopsis

The remote host has a version of Adobe Media Server installed that is no longer supported.

Description

According to its version, the installation of Adobe Media Server (formerly Adobe Flash Media Server) on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Risk Factor

Critical

Plugin Information

Published: 2011/08/11, Modified: 2022/04/11

Plugin Output

tcp/1111/rtmp

```
Version source : FlashCom/4.5.0
Installed version : 4.5.0
Supported version(s) : 5.0
URL : http://www.Soundview Security.org/u?03cbab03
```

100995 - Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.33-dev or 2.4.x prior to 2.4.26. It is, therefore, affected by the following vulnerabilities :

- An authentication bypass vulnerability exists due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167)

- A NULL pointer dereference flaw exists due to third-party module calls to the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169)

- A NULL pointer dereference flaw exists in mod_http2 that is triggered when handling a specially crafted HTTP/2 request. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. Note that this vulnerability does not affect 2.2.x.
(CVE-2017-7659)

- An out-of-bounds read error exists in the ap_find_token() function due to improper handling of header sequences. An unauthenticated, remote attacker can exploit this, via a specially crafted header sequence, to cause a denial of service condition.
(CVE-2017-7668)

- An out-of-bounds read error exists in mod_mime due to improper handling of Content-Type response headers. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type response header, to cause a denial of service condition or the disclosure of sensitive information. (CVE-2017-7679)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2017/06/22, Modified: 2022/04/11

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Installed version : 2.2.17
Fixed version : 2.2.33
```

101787 - Apache 2.2.x < 2.2.34 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.34. It is, therefore, affected by the following vulnerabilities :

- An authentication bypass vulnerability exists in httpd due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167)

- A denial of service vulnerability exists in httpd due to a NULL pointer dereference flaw that is triggered when a third-party module calls the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service

condition. (CVE-2017-3169)

- A denial of service vulnerability exists in httpd due to an out-of-bounds read error in the ap_find_token() function that is triggered when handling a specially crafted request header sequence. An unauthenticated, remote attacker can exploit this to crash the service or force ap_find_token() to return an incorrect value. (CVE-2017-7668)

- A denial of service vulnerability exists in httpd due to an out-of-bounds read error in the mod_mime that is triggered when handling a specially crafted Content-Type response header. An unauthenticated, remote attacker can exploit this to disclose sensitive information or cause a denial of service condition. (CVE-2017-7679)

- A denial of service vulnerability exists in httpd due to a failure to initialize or reset the value placeholder in [Proxy-]Authorization headers of type 'Digest' before or between successive key=value assignments by mod_auth_digest. An unauthenticated, remote attacker can exploit this, by providing an initial key with no '=' assignment, to disclose sensitive information or cause a denial of service condition. (CVE-2017-9788)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2017/07/18, Modified: 2018/09/17

Plugin Output

tcp/80

```
Source : Server: Apache/2.2.17 (Win32) DAV/2
Installed version : 2.2.17
Fixed version : 2.2.34
```

158900 - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.

- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)

- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)

- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)

- Read/write beyond bounds in mod_sed: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Acknowledgements: Ronald Crane (Zippenhop LLC) (CVE-2022-23943)

Note that Soundview Security has not tested for this issue but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2022/03/14, Modified: 2023/11/06

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Installed version : 2.2.17
Fixed version : 2.4.53
```

161948 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Possible request smuggling in mod_proxy_ajp: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions. Acknowledgements: Ricter Z @ 360 Noah Lab (CVE-2022-26377)

- Read beyond bounds in mod_isapi: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28330)

- Read beyond bounds via ap_rwrite(): The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28614)

- Read beyond bounds in ap_strcmp_match(): Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28615)

- Denial of service in mod_lua r:parsebody: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-29404)

- Denial of Service mod_sed: If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort. Acknowledgements: This issue was found by Brian Moussalli from the JFrog Security Research team (CVE-2022-30522)

- Information Disclosure in mod_lua with websockets: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-30556)

- X-Forwarded-For dropped by hop-by-hop mechanism in mod_proxy: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application. Acknowledgements: The Apache HTTP Server project would like to thank Gaetan Ferry (Synacktiv) for reporting this issue (CVE-2022-31813)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2022/06/08, Modified: 2023/10/25

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Installed version : 2.2.17
Fixed version : 2.4.54
```

170113 - Apache 2.4.x < 2.4.55 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.55. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.55 advisory.

- A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier. (CVE-2006-20001)

- Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions. (CVE-2022-36760)

- Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client. (CVE-2022-37436)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)

Plugin Information

Published: 2023/01/18, Modified: 2023/03/10

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Installed version : 2.2.17
Fixed version : 2.4.55
```

172186 - Apache 2.4.x < 2.4.56 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory.

- HTTP request splitting with mod_rewrite and mod_proxy: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule ^/here/(.*) http://example.com:8080/elsewhere?$1 http://example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Acknowledgements: finder: Lars Krapf of Adobe (CVE-2023-25690)

- Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.
Special characters in the origin response header can truncate/split the response forwarded to the client.
Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2023/03/07, Modified: 2023/10/21

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Installed version : 2.2.17
Fixed version : 2.4.56
```

153583 - Apache < 2.4.49 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog.

- A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. (CVE-2021-40438)

Note that Soundview Security has not tested for this issue but has instead relied only on the application's self-reported version number.

Risk Factor

Medium

CVSS v3.0 Base Score

9.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)

Plugin Information

Published: 2021/09/23, Modified: 2023/04/25

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Installed version : 2.2.17
Fixed version : 2.4.49
```

153584 - Apache < 2.4.49 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.49 changelog.

- ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. (CVE-2021-39275)

- Malformed requests may cause the server to dereference a NULL pointer. (CVE-2021-34798)

Note that Soundview Security has not tested for this issue but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2021/09/23, Modified: 2022/04/11

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Installed version : 2.2.17
Fixed version : 2.4.49
```

171356 - Apache HTTP Server SEoL (2.1.x <= x <= 2.2.x) -

Synopsis

An unsupported version of Apache HTTP Server is installed on the remote host.

Description

According to its version, Apache HTTP Server is between 2.1.x and 2.2.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Plugin Information

Published: 2023/02/10, Modified: 2024/04/02

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Installed version : 2.2.17
Security End of Life : July 10, 2017
Time since Security End of Life (Est.) : >= 6 years
```

62101 - Apache 2.2.x < 2.2.23 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.23. It is, therefore, potentially affected by the following vulnerabilities :

- The utility 'apachectl' can receive a zero-length directory name in the LD_LIBRARY_PATH via the 'envvars'
file. A local attacker with access to that utility could exploit this to load a malicious Dynamic Shared Object (DSO), leading to arbitrary code execution.
(CVE-2012-0883)

- An input validation error exists related to 'mod_negotiation', 'Multiviews' and untrusted uploads that can allow cross-site scripting attacks.
(CVE-2012-2687)

Note that Soundview Security has not tested for these flaws but has instead relied on the version in the server's banner.

Risk Factor

Medium

CVSS v3.0 Base Score

7.0 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2012/09/14, Modified: 2018/06/29

Plugin Output

tcp/80

```
Version source : Server: Apache/2.2.17 (Win32) DAV/2
Installed version : 2.2.17
Fixed version : 2.2.23
```

77531 - Apache 2.2.x < 2.2.28 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.28. It is, therefore, affected by the following vulnerabilities :

- A flaw exists within the 'mod_headers' module which allows a remote attacker to inject arbitrary headers.
This is done by placing a header in the trailer portion of data being sent using chunked transfer encoding.
(CVE-2013-5704)

- A flaw exists within the 'mod_deflate' module when handling highly compressed bodies. Using a specially crafted request, a remote attacker can exploit this to cause a denial of service by exhausting memory and CPU resources. (CVE-2014-0118)

- The 'mod_status' module contains a race condition that can be triggered when handling the scoreboard. A remote attacker can exploit this to cause a denial of service, execute arbitrary code, or obtain sensitive credential information. (CVE-2014-0226)

- The 'mod_cgid' module lacks a time out mechanism. Using a specially crafted request, a remote attacker can use this flaw to cause a denial of service by causing child processes to linger indefinitely, eventually filling up the scoreboard. (CVE-2014-0231)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

Medium

CVSS v3.0 Base Score

7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

Plugin Information

Published: 2014/09/04, Modified: 2020/04/27

Plugin Output

tcp/80

```
Version source : Server: Apache/2.2.17 (Win32) DAV/2
Installed version : 2.2.17
Fixed version : 2.2.29
```

183391 - Apache 2.4.x < 2.4.58 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.58 advisory.

- mod_macro buffer over-read: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
Acknowledgements: finder: David Shoon (github/davidshoon) (CVE-2023-31122)

- Apache HTTP Server: DoS in HTTP/2 with initial windows size 0: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known slow loris attack pattern. This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57. Users are recommended to upgrade to version 2.4.58, which fixes the issue.
Acknowledgements: (CVE-2023-43622)

- Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During normal HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue. Acknowledgements: (CVE-2023-45802)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Plugin Information

Published: 2023/10/19, Modified: 2024/04/11

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Installed version : 2.2.17
Fixed version : 2.4.58
```

192923 - Apache 2.4.x < 2.4.59 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.59. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.59 advisory.

- Apache HTTP Server: HTTP Response Splitting in multiple modules: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack. Users are recommended to upgrade to version 2.4.59, which fixes this issue. Acknowledgements: (CVE-2024-24795)

- Apache HTTP Server: HTTP/2 DoS by memory exhaustion on endless continuation frames: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion. Acknowledgements: finder: Bartek Nowotarski (https://nowotarski.info/) (CVE-2024-27316)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Plugin Information

Published: 2024/04/04, Modified: 2024/04/12

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Installed version : 2.2.17
Fixed version : 2.4.59
```

53896 - Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS -

Synopsis

The remote web server may be affected by a denial of service vulnerability.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.18. It is, therefore, affected by a denial of service vulnerability due to an error in the apr_fnmatch() function of the bundled APR library.

If mod_autoindex is enabled and has indexed a directory containing files whose filenames are long, an attacker can cause high CPU usage with a specially crafted request.

Note that the remote web server may not actually be affected by this vulnerability. Soundview Security did not try to determine whether the affected module is in use or to check for the issue itself.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Plugin Information

Published: 2011/05/13, Modified: 2018/06/29

Plugin Output

tcp/80

```
Version source : Server: Apache/2.2.17 (Win32) DAV/2
Installed version : 2.2.17
Fixed version : 2.2.18
```

56216 - Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS -

Synopsis

The remote web server is affected by a denial of service vulnerability.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.21. It is, therefore, potentially affected by a denial of service vulnerability. An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.

Note that Soundview Security did not actually test for the flaws but instead has relied on the version in the server's banner.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Plugin Information

Published: 2011/09/16, Modified: 2018/06/29

Plugin Output

tcp/80

```
Version source : Server: Apache/2.2.17 (Win32) DAV/2
Installed version : 2.2.17
Fixed version : 2.2.21
```

57791 - Apache 2.2.x < 2.2.22 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x installed on the remote host is prior to 2.2.22. It is, therefore, potentially affected by the following vulnerabilities :

- When configured as a reverse proxy, improper use of the RewriteRule and ProxyPassMatch directives could cause the web server to proxy requests to arbitrary hosts.
This could allow a remote attacker to indirectly send requests to intranet servers.
(CVE-2011-3368, CVE-2011-4317)

- A heap-based buffer overflow exists when mod_setenvif module is enabled and both a maliciously crafted 'SetEnvIf' directive and a maliciously crafted HTTP request header are used. (CVE-2011-3607)

- A format string handling error can allow the server to be crashed via maliciously crafted cookies.
(CVE-2012-0021)

- An error exists in 'scoreboard.c' that can allow local attackers to crash the server during shutdown.
(CVE-2012-0031)

- An error exists in 'protocol.c' that can allow 'HTTPOnly' cookies to be exposed to attackers through the malicious use of either long or malformed HTTP headers.
(CVE-2012-0053)

- An error in the mod_proxy_ajp module when used to connect to a backend server that takes an overly long time to respond could lead to a temporary denial of service. (CVE-2012-4557)

Note that Soundview Security did not actually test for these flaws, but instead has relied on the version in the server's banner.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Plugin Information

Published: 2012/02/02, Modified: 2018/06/29

Plugin Output

tcp/80

```
Version source : Server: Apache/2.2.17 (Win32) DAV/2
Installed version : 2.2.17
Fixed version : 2.2.22
```

64912 - Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities -

Synopsis

The remote web server is affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.24. It is, therefore, potentially affected by the following cross-site scripting vulnerabilities :

- Errors exist related to the modules mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp and unescaped hostnames and URIs that could allow cross- site scripting attacks. (CVE-2012-3499)

- An error exists related to the mod_proxy_balancer module's manager interface that could allow cross-site scripting attacks. (CVE-2012-4558)

Note that Soundview Security did not actually test for these issues, but instead has relied on the version in the server's banner.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Plugin Information

Published: 2013/02/27, Modified: 2018/06/29

Plugin Output

tcp/80

```
Version source : Server: Apache/2.2.17 (Win32) DAV/2
Installed version : 2.2.17
Fixed version : 2.2.24
```

68915 - Apache 2.2.x < 2.2.25 Multiple Vulnerabilities -

Synopsis

The remote web server may be affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists in the 'RewriteLog' function where it fails to sanitize escape sequences from being written to log files, making it potentially vulnerable to arbitrary command execution. (CVE-2013-1862)

- A denial of service vulnerability exists relating to the 'mod_dav' module as it relates to MERGE requests.
(CVE-2013-1896)

Note that Soundview Security did not actually test for these issues, but instead has relied on the version in the server's banner.

Risk Factor

Medium

CVSS v3.0 Base Score

5.6 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)

Plugin Information

Published: 2013/07/16, Modified: 2018/06/29

Plugin Output

tcp/80

```
Version source : Server: Apache/2.2.17 (Win32) DAV/2
Installed version : 2.2.17
Fixed version : 2.2.25
```

73405 - Apache 2.2.x < 2.2.27 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is a version prior to 2.2.27. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists with the 'mod_dav' module that is caused when tracking the length of CDATA that has leading white space. A remote attacker with a specially crafted DAV WRITE request can cause the service to stop responding.
(CVE-2013-6438)

- A flaw exists in 'mod_log_config' module that is caused when logging a cookie that has an unassigned value. A remote attacker with a specially crafted request can cause the service to crash. (CVE-2014-0098)

Note that Soundview Security did not actually test for these issues, but instead has relied on the version in the server's banner.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Plugin Information

Published: 2014/04/08, Modified: 2018/09/17

Plugin Output

tcp/80

```
Version source : Server: Apache/2.2.17 (Win32) DAV/2
Installed version : 2.2.17
Fixed version : 2.2.27
```

88098 - Apache Server ETag Header Information Disclosure -

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Plugin Information

Published: 2016/01/22, Modified: 2020/04/27

Plugin Output

tcp/80

```
Soundview Security was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

Source : ETag: "700000001e5ca-64dc-4ab59cd8f4400"
Inode number : 124362
File size : 25820 bytes
File modification time : Aug. 25, 2011 at 19:54:56 GMT
```

10678 - Apache mod_info /server-info Information Disclosure -

Synopsis

The remote web server discloses configuration information.

Description

A remote unauthenticated attacker can obtain an overview of the remote Apache web server's configuration by requesting the URL '/server-info'. This overview includes information such as installed modules, their configuration, and assorted run-time settings.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Plugin Information

Published: 2001/05/28, Modified: 2018/08/09

Plugin Output

tcp/80

```
Soundview Security was able to exploit the issue to retrieve the contents of
'server-status' using the following request :

http://x.x.1.26/server-info

Attached is a copy of the response
```

10677 - Apache mod_status /server-status Information Disclosure -

Synopsis

The remote web server discloses process information.

Description

A remote unauthenticated attacker can obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Plugin Information

Published: 2001/05/28, Modified: 2018/08/09

Plugin Output

tcp/80

```
Soundview Security was able to exploit the issue to retrieve the contents of
'server-status' using the following request :

http://x.x.1.26/server-status

Attached is a copy of the response
```

11213 - HTTP TRACE / TRACK Methods Allowed -

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

Plugin Output

tcp/80

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Soundview Security sent the following TRACE request : \n\n------------------------------ snip ---------------------------
---\nTRACE /Soundview Security1935916612.html HTTP/1.1
Connection: Close
Host: x.x.1.26
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n\nand received the following response from the remote
server :\n\n------------------------------ snip ------------------------------\nHTTP/1.1 200 OK
Date: Mon, 16 Apr 2024 11:59:01 GMT
Server: Apache/2.2.17 (Win32) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Soundview Security1935916612.html HTTP/1.1
```

```
Connection: Keep-Alive
Host: x.x.1.26
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n
```

50705 - Adobe Flash Media Server Version Detection -

Synopsis

The remote web server reports its version number in HTTP headers.

Description

Adobe Flash Media Server, a data and media server that serves applications to Flash Player, appears to be running on the remote host and is reporting its version number in HTTP headers.

Risk Factor

None

Plugin Information

Published: 2010/11/24, Modified: 2019/11/22

Plugin Output

tcp/1111/rtmp

```
Version source : FlashCom/4.5.0
Installed version : 4.5.0
```

50705 - Adobe Flash Media Server Version Detection -

Synopsis

The remote web server reports its version number in HTTP headers.

Description

Adobe Flash Media Server, a data and media server that serves applications to Flash Player, appears to be running on the remote host and is reporting its version number in HTTP headers.

Risk Factor

None

Plugin Information

Published: 2010/11/24, Modified: 2019/11/22

Plugin Output

tcp/1935

```
Version source : FlashCom/4.5.0
Installed version : 4.5.0
```

48204 - Apache HTTP Server Version -

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Risk Factor

None

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80

```
URL : http://x.x.1.26/
Version : 2.2.17
Source : Server: Apache/2.2.17 (Win32) DAV/2
backported : 0
modules : DAV/2
os : Win32
```

45590 - Common Platform Enumeration (CPE) -

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Soundview Security scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/04/03

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:microsoft:windows -> Microsoft Windows

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.2.17 -> Apache Software Foundation Apache HTTP Server
cpe:/a:jquery:jquery:1.5.1 -> jQuery
```

54615 - Device Type -

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : embedded
Confidence level : 59
```

10092 - FTP Server Detection -

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80

```
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

/
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Risk Factor

None

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80

```
The remote web server type is :

Apache/2.2.17 (Win32) DAV/2
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Headers :

Date: Mon, 16 Apr 2024 12:02:32 GMT
Server: Apache/2.2.17 (Win32) DAV/2
Last-Modified: Thu, 25 Aug 2011 19:54:56 GMT
ETag: "700000001e5ca-64dc-4ab59cd8f4400"
Accept-Ranges: bytes
Content-Length: 25820
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Response Body :

<!--
/*
* (C) Copyright 2011 Adobe Systems Incorporated. All Rights Reserved.
*
* NOTICE: Adobe permits you to use, modify, and distribute this file in accordance with the
* terms of the Adobe license agreement accompanying it. If you have received this file from a
* source other than Adobe, then your use, modification, or distribution of it requires the prior
* written permission of Adobe.
* THIS CODE AND INFORMATION IS PROVIDED "AS-IS" WITHOUT WARRANTY OF
* ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO
* THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A
* PARTICULAR PURPOSE.
*
* THIS CODE IS NOT SUPPORTED BY Adobe Systems Incorporated.
*
*/
-->

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<!-- saved from url=(0014)about:internet -->
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
```

```
<title>Adobe Flash Media Server</title>
<link rel="stylesheet" type="text/css" href="startpage.css" />
<!-- Enable Browser History by replacing useBrowserHistory tokens with two hyphens -->
<!-- BEGIN Browser History required section -->
<link rel="stylesheet" type="text/css" href="history/history.css" />
<style type="text/css" media="screen">
html, body { height:100%; }
body { margin:0;
padding:0;
overflow:auto;
text-align:center;
background-color: #000000;
}
object:focus { outline:none; }
#flashContent { display:none; }
</style>
<script type="text/javascript" src="history/history.js"></script>
<!-- END Browser History required section -->

<script type="text/javascript" src="scripts/swfobject.js"></script>
<script type="text/javascript" src="scripts/jquery-1.5.1.min.js"></script>
<script type="text/javascript">
function loadLinks() {
var hostName = window.location.hostname;
var portNum = window.location.port.toString();
if(hostName.length > 0)
{
hostName = "http://" + hostName;
if (portNum.length > 0)
hostName += ":" + portNum;
}
else
{
hostName = "http://localhost";
if (portNum.length > 0)
hostName += ":" + portNum;
}
var sourceURL = new String(document.location.href);
var paramsIndex = sourceURL.indexOf("?");
if (paramsIndex != -1) {
sourceURL = sourceURL.substring(0, paramsIndex);
}
sourceURL = sourceURL.substring(sourceURL.lastIndexOf("/") + 1);

// Update links

var link;
link = "&protocol=rtmp&protection=RTMPe&xml=rtmp";
$("a.rtmpsingle").click(function(e){ preloadSWF("url=rtmp:/vod/mp4:sample1_1500kbps.f4v" + link + "&type=rtmpsingle") });
$("a.rtmpmbr").click(function(e){ preloadSWF("url=" + hostName + "/vod/rtmp_sample1_manifest.f4m" + link +
"&type=rtmpmbr") });

link = "&protocol=HTTP&protection=None&xml=http";
$("a.httpsingle").click(function(e){ preloadSWF("url=" + hostName + "/hds-vod/sample1_1500kbps.f4v.f4m" + link +
"&type=httpsingle") });
$("a.httpmbr").click(function(e){ preloadSWF("url=" + hostName + "/vod/hds_sample1_manifest.f4m" + link +
"&type=httpmbr") });

link = "&protocol=HTTP&protection=None&xml=hls";
$("a.hlssingle").click(function(e){ preloadSWF("url=" + hostName + "/hls-vod/sample1_1500kbps.f4v.m3u8" + link +
"&type=hlssingle") });
$("a.hlsmbr").click(function(e){ preloadSWF("url=" + hostName + "/vod/hls_sample1_manifest.m3u8" + link + "&type=hlsmbr")
});
}

$(document).ready(function(){

loadLinks();

$('#streaming_tab').click(function(e){
$(this).removeClass('streaming_tab_normal').addClass('streaming_tab_selected');
$('#interactive_tab').removeClass('interactive_tab_selected').addClass('interactive_tab_normal');
$("#streaming_content").removeClass('nav_content_hide').addClass('nav_content_show');
$('#interactive_content').removeClass('nav_content_show').addClass('nav_content_hide');

});
$('#interactive_tab').click(function(e){
loadSWF("swfs/LiveSample.swf", 640, 377);
$(this).removeClass('interactive_tab_normal').addClass('interactive_tab_selected');
$("#streaming_tab").removeClass('streaming_tab_selected').addClass('streaming_tab_normal');
$("#interactive_content").removeClass('nav_content_hide').addClass('nav_content_show');
$('#streaming_content').removeClass('nav_content_show').addClass('nav_content_hide');
});

var currentURL = new String(document.location.href);
var params = unescape(currentURL.substring(indexOfParams + 1));
var indexOfParams = currentURL.indexOf("?");

if (indexOfParams != -1) {
preloadSWF(params);
} else {
preloadSWF();
}

});

function preloadSWF(params)
{
```

```
// Figure out which swf to embed.

var source = (params) ? params : "url=rtmp:/vod/mp4:sample1_1500kbps.f4v&protocol=rtmp&xml=rtmp&type=rtmpsingle";

var uagent = navigator.userAgent.toLowerCase();
var swfURL = "swfs/adobedemoplayer_pc.swf";
var swfWidth = "770";
var swfHeight = "457";
var embedSWF = true;
var ignoreHTML5 = false;
var embedWmode = "direct";
var secondIdx;

var urlParam = "url=";
var urlIdx = source.indexOf(urlParam);
var url;

if (urlIdx != -1) {
secondIdx = source.indexOf("&", urlIdx);
if (secondIdx != -1) {
url = source.substring(urlIdx + urlParam.length, secondIdx);
}
else {
url = source.substring(urlIdx + urlParam.length);
}

var sepIdx = url.lastIndexOf(".");
if (sepIdx != -1) {
var type = url.substring(sepIdx+1);
if (type == "m3u8") {
embedSWF = false;
}
}
}

if (embedSWF) {
loadSWF(swfURL, swfWidth, swfHeight, embedWmode, url);
if (uagent.search('iphone') != -1 || uagent.search('ipad') != -1) {
var htmlData = $("#player_main").html();
$("#player_main").html(htmlData + "<p style='font-size:24px;margin-top:100px;'>Flash is currently not available for this
device.<br /> Please use the (HLS) HTTP Live Streaming links to the right.</p>");
}
}
else {
$("#html5_vid").show();
var ele = document.getElementById("demoPlayer");
if (ele && (ele.nodeName === "OBJECT" || ele.nodeName === "EMBED"))
{
var div = document.createElement("div");
ele.parentNode.insertBefore(div, ele);
swfobject.removeSWF("demoPlayer");
div.setAttribute("id", "player_main");
}
if (uagent.search('firefox') != -1 || uagent.search('chrome') != -1 || uagent.search('msie') != -1) {
$("#html5_vid").hide();
$("#player_main").html("<p style='font-size:20px;margin-top:150px;'>This browser is not capable of playing the HTML5
video.<br /> Please use an Apple Safari browser with HTML5 video support.</p>");
ignoreHTML5 = true;
}
else
{
swfobject.createCSS("#player_main", "display:none;");
}
}

// reset the buttons to the top position
$("a.rtmpsingle").css("background-position","top");
$("a.httpsingle").css("background-position","top");
$("a.hlssingle").css("background-position","top");
$("a.rtmpmbr").css("background-position","top");
$("a.httpmbr").css("background-position","top");
$("a.hlsmbr").css("background-position","top");

var items = source.split("&");
var xml;

for ( var i = 0; i < items.length; i++ ) {
var p = items[i];
var pieces = p.split("=");
switch ( pieces[0] ) {
case "type":
xml = pieces[1];
// Highlight the matching navigation button.
switch ( xml ) {
case "rtmpsingle":
$("a.rtmpsingle").css("background-position","bottom");
break;
case "httpsingle":
$("a.httpsingle").css("background-position","bottom");
break;
case "hlssingle":
$("a.hlssingle").css("background-position","bottom");
break;
case "rtmpmbr":
$("a.rtmpmbr").css("background-position","bottom");
break;
case "httpmbr":
$("a.httpmbr").css("background-position","bottom");
```

```
break;
case "hlsmbr":
$("a.hlsmbr").css("background-position","bottom");
break;
}
break;
case "url":
if (ignoreHTML5 == false) {
$("video.videoplayer").attr( "src", pieces[1] );
}
break;
}
}

}



function loadSWF(swfURL, swfWidth, swfHeight, swfMode, src)
{
$("#html5_vid").hide();
var ele = document.getElementById("demoPlayer");
if (ele && (ele.nodeName === "OBJECT" || ele.nodeName === "EMBED"))
{
var div = document.createElement("div");
ele.parentNode.insertBefore(div, ele);
swfobject.removeSWF("demoPlayer");
div.setAttribute("id", "player_main");
}

$("div.player_window").css("width", String("770px"));
$("div.player_window").css("height", String("457px"));
$("div.player_window").css("text-align", "center");

// For version detection, set to min. required Flash Player version, or 0 (or 0.0.0), for no version detection.
var swfVersionStr = "10.2.0";
// To use express install, set to playerProductInstall.swf, otherwise the empty string.
var xiSwfUrlStr = "swfs/playerProductInstall.swf";
var flashvars = {};
if (src)
{
flashvars.src = src;
}
var params = {};
params.quality = "high";
params.bgcolor = "#000000";
params.allowscriptaccess = "sameDomain";
params.allowfullscreen = "true";
params.wmode = swfMode;
var attributes = {};
attributes.id = "demoPlayer";
attributes.name = "demoPlayer";
attributes.align = "middle";
swfobject.embedSWF(
swfURL, "player_main",
swfWidth, swfHeight,
swfVersionStr, xiSwfUrlStr,
flashvars, params, attributes);
swfobject.createCSS("player_main", "display:inline;text-align:center;outline:none;border:0;vertical-align:middle;margin:0
auto;");

}

function troubleshooting() {
alert("Flash Media Server ships with sample f4m manifest files. These files are coded to operate using the \"localhost\"
server. To access the server remotely, you will need to replace the localhost reference with your actual server name or
IP Address. \n\nFollow these steps:\n" +

"1. Locate the files Manifest files. Browse to [serverinstall]/webroot/vod\n" +
"2. Backup the 2 f4m manifest files\n" +
"\ta. hds_sample1_manifest.f4m\n" +
"\tb. rtmp_sample1_manifest.f4m\n" +
"3. Edit the original files using a text editor.\n" +
"4. Replace the \"localhost\" references with the name or IP address of your server\n" +
"5. On your remote device, you may need to clear the browser cache\n" +
"6. Reload the start page, and your video should play\n\n" +

"Note: this is not required for HLS playback, the M3u8 supports the relative URI path.\n");
}
</script>
</head>

<body>
<div class="content">
<!--


Title and Links


-->
<div class="title_banner"><a class="fms_logo" href="http://www.adobe.com/go/fms" target="_blank"></a> <a
class="adobe_logo_tag" href="http://www.adobe.com" target="_blank"></a>
<div class="header_links"> <a class="header_link" target="_blank"
href="http://www.adobe.com/go/flashmediaserver_wishform_en">Request A Feature</a> <a class="header_link" target="_blank"
href="http://www.adobe.com/go/flashmediaserver_wishform_en">Submit A Bug</a> <a class="header_link" target="_blank"
href="http://www.adobe.com/go/flashmediaserver_releasenotes_en">Release Notes</a> <a class="header_link" target="_blank"
href="http://www.adobe.com/go/flashmediaserver_docs_en">Documentation</a> <a class="header_link" target="_blank"
```

```
href="http://www.adobe.com/go/gpr_registration">Register</a> </div>
</div>

<!--


Splash Banner


-->
<div class="content_banner">
<div class="content_banner_text"></div>
<div class="fms_mnemonic"></div>
<a class="content_banner_button content_banner_admin_button" target="_blank" href="fms_adminConsole.htm"></a> <a
class="content_banner_button content_banner_update_button" target="_blank" href="http://www.adobe.com/go/fms_updates">
</a>
</div>

<table class="player_region" cellpadding="0" cellspacing="0"><tr>
<!--


Player Windows


-->
<td width="770" valign="top"><div class="player_window">
<div id="html5_vid">
<video id="vid_player" class="videoplayer" controls="controls" autoplay="autoplay"> This browser does not support the
video tag. </video>
</div>
<div id="player_main" align="center" style="text-align: center;vertical-align:middle;">
<img src="images/no_flash_title.png"
alt="This video requires Adobe Flash Player 10.2" style="margin:10px auto;vertical-align:middle;"/>
<div style="text-align:center;" align="center">
<a href="http://www.adobe.com/go/getflashplayer">Download Flash Player</a><br />
<script type="text/javascript">
var pageHost = ((document.location.protocol == "https:") ? "https://" : "http://");
document.write("<a href='http://www.adobe.com/go/getflashplayer'><img src='" + pageHost +
"www.adobe.com/images/shared/download_buttons/get_flash_player.gif' alt='Get Adobe Flash player' /></a>");
</script>
</div>
</div>
</div>
</td>
<!--


Navigation Panel


-->
<td width="218" valign="top"><div class="nav_tabs">
<div id="streaming_tab" class="tabs streaming_tab_selected">Streaming</div>
<div id="interactive_tab" class="tabs interactive_tab_normal">Interactive</div>
<div id="streaming_content" class="nav_content nav_content_show">
<div class="troubleshooting" onclick="troubleshooting()">Troubleshooting Playback</div>
<div class="nav_hrule"></div>
<p class="nav_header">(HDS) HTTP DYNAMIC<br clear="all"/>
STREAMING SAMPLE</p>
<p class="nav_note">requires Apache server to be installed</p>
<p class="nav_link"><a class="play_button two_state_button httpmbr"></a> <a class="play_link httpmbr">HDS Multiple
Bitrate</a></p>
<p class="nav_link"><a class="play_button two_state_button httpsingle"></a> <a class="play_link httpsingle">HDS Single
Bitrate</a></p>
<div class="nav_hrule"></div>
<p class="nav_header">RTMP DYNAMIC
STREAMING SAMPLE</p>
<p class="nav_link"><a class="play_button two_state_button rtmpmbr"></a> <a class="play_link rtmpmbr"> Multiple
Bitrate</a></p>
<p class="nav_link"><a class="play_button two_state_button rtmpsingle"></a> <a class="play_link rtmpsingle">Single
Bitrate</a></p>
<div class="nav_hrule"></div>
<p class="nav_header">(HLS) HTTP LIVE<br clear="all"/>
STREAMING FOR APPLE IOS</p>
<p class="nav_note">requires Apache server to be installed</p>
<p class="nav_link"><a class="play_button two_state_button hlsmbr"></a> <a class="play_link hlsmbr"> Multiple Bitrate</a>
</p>
<p class="nav_link"><a class="play_button two_state_button hlssingle"></a> <a class="play_link hlssingle">Single
Bitrate</a></p>
</div>
<div id="interactive_content" class="nav_content nav_content_hide" style="padding: 10px 10px 10px 10px;">
<p>USE YOUR WEBCAM<br /> TO STREAM A LIVE VIDEO</p>
<p>If you have a camera installed, you can publish it to Flash Media Server.<br />
When you click Publish, your camera feed will be published to Flash Media Server.<br />
When you click the Play button, the stream will be received from Flash Media Server.</p>
<br />
<p>TIP: You can use the window on the right to receive any live stream from Flash Media Server.</p>


</div>
</div>
</td>
</tr></table>
<div class="hrule"></div>
<div class="additional_info">
<table width="960" border="0" cellspacing="0" cellpadding="0" class="additional_resources_table">
<tr>
```

<th valign="bottom" style="width: 325px;">TOOLS</th>
<th valign="bottom" style="width: 305px;">SAMPLE APPLICATIONS
AND WHITE PAPERS </th>
<th valign="bottom" style="width: 300px;">GETTING STARTED</th>
</tr>
<tr>
<!--

Tools Column

-->
<td valign="top" style="width: 325px;">

Flash Media Playback Configurator
Easy to use media player that requires no client development, just configure it, add your manifest file and you can start streaming quickly.
Strobe Media Playback with Debug
Prebuilt video player interface and source code to accelerate your custome video player development. For troubleshooting, the Strobe Media Playback debug player is available at http://www.osmf.org/dev.
Open Source Media Framework
Robust media player development using OSMF optimized for HDS, RTMP, Multicast, P2P and adaptive bitrate. You can also easily use external services like advertising and analytics easily.
Manifest Generator for HTTP Streaming
Generate manifest files easier and with fewer errors with tools that cut out creating F4M and M3u8 files manually for Live and VOD delivery for Flash, and for Apple iOS. Located in the folder: /tools
Manifest Generator for Multicast
Generate multicast, multicast fusion and P2P manifest files easier and with fewer errors with tools that cut out creating F4M manually for multicast streaming to Flash. Located in the folder: /tools
FLVCheck Tool
Ensure video files are compatible to stream with FMS. Use it as-is, or as part of an automated script.
Other Productivity Tools
Additional productivity tools are available on http://www.adobe.com/go/fms_tools including server applications such as FMSCheck, DVRCast, and LiveStreamCast.
</td>
<!--

Sample Apps Column

-->
<td valign="top">

 Flash Media Server 4.5 Whitepaper
Everything you need to know about Flash Media Server 4.5.
HTTP Dynamic Streaming Whitepaper

Full details for HTTP Dynamic Streaming are available for complete understanding how it works, and how to optimize.

Large Scale Deployments
Learn how to configure Flash Media Server for large-scale enterprise deployments.
Security: Server Hardening Guide
Learn how to deploy your Flash Media Server safely and securely.
F4V/F4F Format Spec
Learn more details about the F4F and F4V File Format used for HTTP Dynamic Streaming.
RTMP Specification
Learn more details about the RTMP protocol for streaming and communication applications.
Calculating Bandwidth
Learn how to calculate how much bandwidth you need to stream video.
Transition guide for Windows Media Server users
Ease the transition from Microsoft Windows Media to Adobe Flash Platform and its related technologies.
</td>
<!--

Getting Started

-->
<td valign="top">

 Developer Connection
P2P / RTMFP Technology
Streaming Recorded Video
Streaming Live Video
Protecting Video
The built-in Web Server

<!--

Getting Support

```
-->
<div class="info_block" style="margin-bottom:0px;">GETTING SUPPORT</div>
<div class="column_rule"></div>
<div class="info_block"> <a href="http://www.adobe.com/go/fms_experts" target="_blank">Find an Expert</a><br />
<a href="http://www.adobe.com/go/flashmediaserver_support_en" target="_blank">Knowledge Base</a><br />
<a href="http://www.adobe.com/go/flashmediaserver_forum_en" target="_blank">Flash Media Discussion Forums</a><br />
<a href="http://adobe.com/go/fms_usergroup" target="_blank">User Groups / Community</a><br />
<a href="http://www.adobe.com/go/flashmediaserver_support_en" target="_blank">Adobe Support for Flash Media Server</a><br
/>
<a href="http://www.adobe.com/events/main.jsp" target="_blank">Worldwide Events</a><br />
<a href="http://www.adobe.com/go/fms_training" target="_blank">Hands on (Instructor-Led) Training</a><br />
<a href="http://www.adobe.com/go/fvss/" target="_blank">CDN Partners</a><br />
<a href="http://www.adobe.com/go/fmsp_consulting/" target="_blank">Consulting Partners</a><br />
<a href="http://www.adobe.com/go/fmsp_encoding/" target="_blank">Encoding Partners</a><br />
<a href="http://www.adobe.com/go/fmsp_publishing/" target="_blank">Publishing Partners</a><br />
<a href="http://www.adobe.com/go/fmsp_addelivery/" target="_blank">Advertising Partners</a><br />
</div>
</td>
</tr>
</table>
</div>
<div class="hrule"></div>
<div class="productsheader"> <a href="http://www.adobe.com/go/fms" target="_blank" class="morelink
two_state_button">More</a> </div>
<div class="products">
<div class="hrule"></div>
<a href="http://www.adobe.com/go/fms" target="_blank" class="productcell fmslink">Adobe Flash Media Server</a>
<div class="hrule"></div>
<a href="http://www.adobe.com/go/flashaccess" target="_blank" class="productcell accesslink">Adobe Flash Access</a>
<div class="hrule"></div>
<a href="http://www.adobe.com/products/adobepass/" target="_blank" class="productcell passlink">Adobe Pass</a>
<div class="hrule"></div>
<a href="http://www.adobe.com/go/fmsaws" target="_blank" class="productcell fmsawslink">Adobe Flash Media Server on
Amazon Web Services</a>
<div class="hrule"></div>
<a href="http://www.adobe.com/products/flashplayer/" target="_blank" class="productcell flashplayerlink">Adobe Flash
Player</a>
<div class="hrule"></div>
<a href="http://www.adobe.com/products/air/" target="_blank" class="productcell airlink">Adobe AIR for devices</a>
<div class="hrule"></div>
<a href="http://www.osmf.org/configurator/fmp/" target="_blank" class="productcell playbacklink">Adobe Flash Media
Playback</a>
<div class="hrule"></div>
<a href="http://www.osmf.org/" target="_blank" class="productcell osmflink">Open Source Media Framework</a>
<div class="hrule"></div>
</div>
<div class="footer">
<p class="footertext">Copyright &copy; 2011 Adobe Systems Incorporated. All rights reserved.</p>
</div>
</div>

</body>
</html>
```

106658 - JQuery Detection -

Synopsis

The web server on the remote host uses JQuery.

Description

Soundview Security was able to detect JQuery on the remote host.

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

tcp/80

```
URL : http://x.x.1.26/scripts/jquery-1.5.1.min.js
Version : 1.5.1
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/80

```
Port 80/tcp was found to be open
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/1111/rtmp

```
Port 1111/tcp was found to be open
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/1935

```
Port 1935/tcp was found to be open
```

19506 - Soundview Security Scan Information -

Synopsis

This plugin displays information about the Soundview Security scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Soundview Security or Soundview Security Home).
- The version of the Soundview Security Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/03/13

Plugin Output

tcp/0

```
Information about this scan :

Soundview Security version : 10.7.2
Soundview Security build : 20029
Plugin feed version : 202404150829
Scanner edition used : Soundview Security
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.126
Port scanner(s) : Soundview Security_syn_scanner
Port range : default
Ping RTT : 383.971 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Soundview Security Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/4/15 16:30 West Asia Standard Time
Scan duration : 912 sec
Scan for malware : no
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Dell EMC VMX
Microsoft Windows Embedded Standard 7
Confidence level : 59
Method : SinFP

The remote host is running one of these operating systems :
Dell EMC VMX
Microsoft Windows Embedded Standard 7
```

66334 - Patch Report -

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/04/09

Plugin Output

tcp/0

```
. You need to take the following action :

[ Apache 2.4.x < 2.4.59 Multiple Vulnerabilities (192923) ]
```

```
+ Action to take : Upgrade to Apache version 2.4.59 or later.
+Impact : Taking this action will resolve 50 different vulnerabilities (CVEs).
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Soundview Security was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Soundview Security was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/1111/rtmp

```
Flash Media Server is running on this port.
```

25220 - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

10287 - Traceroute Information -

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.126 to x.x.1.26 :
192.168.0.126
192.168.0.234
39.37.128.1
10.253.9.38
10.253.8.98
10.253.4.36
?
116.51.17.201
180.87.108.162
?
63.243.180.64
?
209.58.86.18
66.198.101.133
?
63.243.128.28
63.243.128.26
209.58.18.65
209.58.60.114
x.x.1.1
x.x.1.26
?
x.x.1.26

Hop Count: 27
```

32318 - Web Site Cross-Domain Policy File Detection -

Synopsis

The remote web server contains a 'crossdomain.xml' file.

Description

The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.

Risk Factor

None

Plugin Information

Published: 2008/05/15, Modified: 2022/04/11

Plugin Output

tcp/80

```
Soundview Security was able to obtain a cross-domain policy file from the remote
host using the following URL :

http://x.x.1.26/crossdomain.xml
```

x.x.1.38

2	0	1	0	13
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Tue Apr 16 16:29:55 2024

End time: Tue Apr 16 16:46:41 2024

Host Information

IP: x.x.1.38

OS: Microsoft Windows Server 2003

Vulnerabilities

97994 - Microsoft IIS 6.0 Unsupported Version Detection -

Synopsis

An unsupported version of Microsoft IIS is running on the remote Windows host.

Description

According to its self-reported version number, the installation of Microsoft Internet Information Services (IIS) 6.0 on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Plugin Information

Published: 2017/04/17, Modified: 2020/09/22

Plugin Output

tcp/80/www

```
Installed version : 6.0
Supported versions : 7.0 or later
EOL date : 2015/07/14
EOL URL : http://www.Soundview Security.org/u?d99a8431
```

34460 - Unsupported Web Server Detection -

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Risk Factor

High

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Plugin Information

Published: 2008/10/21, Modified: 2023/02/10

Plugin Output

tcp/80/www

```
Product : Microsoft IIS 6.0
Server response header : Microsoft-IIS/6.0
Support ended : 2015-07-14
Supported versions : Microsoft IIS 8.5 / 8.0
Additional information : http://www.Soundview Security.org/u?d8353958
```

11714 - Nonexistent Page (404) Physical Path Disclosure -

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server reveals the physical path of the webroot when a nonexistent page is requested.

While printing errors to the output is useful for debugging applications, this feature should be disabled on production servers.

Risk Factor

Medium

Plugin Information

Published: 2003/06/11, Modified: 2018/06/27

Plugin Output

tcp/80/www

```
URL : http://x.x.1.38/niet80794135.aspx
Path disclosed : C:\ProdProjects\MTV\MTV 2013-08-26\
Response snippet :
------------------------------ snip ------------------------------
</html>

<!--

[FileNotFoundException]: C:\ProdProjects\MTV\MTV 2013-08-26\niet80794135.aspx

at System.Web.UI.TemplateParser.GetParserCacheItem()

at System.Web.UI.TemplateControlParser.CompileAndGetParserCacheItem(String virtualPath, String inputFile, HttpContext
context)


------------------------------ snip ------------------------------
```

45590 - Common Platform Enumeration (CPE) -

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Soundview Security scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/04/03

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:microsoft:windows_2003_server -> Microsoft Windows Server 2003

Following application CPE matched on the remote system :

cpe:/a:microsoft:iis:6.0 -> Microsoft IIS
```

54615 - Device Type -

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 75
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD TRACE OPTIONS are allowed on :

/
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Risk Factor

None

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Microsoft-IIS/6.0
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

Date: Mon, 16 Apr 2024 11:34:14 GMT
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Set-Cookie: XYZTest=1; path=/
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: -1
Content-Type: text/html; charset=utf-8
Content-Length: 627

Response Body :



<html>
<head>
<title>VIACOM Black Car Reservation System - Powered by SmartCab Corporate!</title>
<script language="JavaScript" src="Script/Utils.js"></script>
<noScript>
<meta http-equiv="refresh" content="0;Url=JSError.aspx">
</noScript>
</head>
<Script language=javascript>
```

```
if (document.title)
{
window.onload=onload=showText;

}

if(document.cookie.indexOf("XYZTest")==-1)
{
location.href="CookieError.aspx";
}
</Script>
<FRAMESET rows="100%,0%" border=0 frameborder=0 >
<FRAME src="Home.aspx" scrolling=auto>
</FRAMESET>
</html>
```

24242 - Microsoft .NET Handlers Enumeration -

Synopsis

It is possible to enumerate the remote .NET handlers used by the remote web server.

Description

It is possible to obtain the list of handlers the remote ASP.NET web server supports.

Risk Factor

None

Plugin Information

Published: 2007/01/26, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
The remote extensions are handled by the remote ASP.NET server :

- .rem
- .soap
```

11874 - Microsoft IIS 404 Response Service Pack Signature -

Synopsis

The remote web server is running Microsoft IIS.

Description

The Patch level (Service Pack) of the remote IIS server appears to be lower than the current IIS service pack level. As each service pack typically contains many security patches, the server may be at risk.

Note that this test makes assumptions of the remote patch level based on static return values (Content-Length) within a IIS Server's 404 error message. As such, the test can not be totally reliable and should be manually confirmed.

Note also that, to determine IIS6 patch levels, a simple test is done based on strict RFC 2616 compliance. It appears as if IIS6-SP1 will accept CR as an end-of-line marker instead of both CR and LF.

Risk Factor

None

Plugin Information

Published: 2003/10/09, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The remote IIS server *seems* to be Microsoft IIS 6.0 - SP1
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

19506 - Soundview Security Scan Information -

Synopsis

This plugin displays information about the Soundview Security scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Soundview Security or Soundview Security Home).
- The version of the Soundview Security Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/03/13

Plugin Output

tcp/0

```
Information about this scan :

Soundview Security version : 10.7.2
Soundview Security build : 20029
Plugin feed version : 202404150829
Scanner edition used : Soundview Security
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.126
Port scanner(s) : Soundview Security_syn_scanner
Port range : default
Ping RTT : 382.912 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
```

```
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Soundview Security Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/4/15 16:30 West Asia Standard Time
Scan duration : 989 sec
Scan for malware : no
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2003
Confidence level : 75
Method : HTTP

The remote host is running Microsoft Windows Server 2003
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Soundview Security was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

25220 - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

10287 - Traceroute Information -

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.126 to x.x.1.38 :
192.168.0.126
192.168.0.234
39.37.128.1
10.253.9.42
10.253.8.14
10.253.4.16
10.253.4.2
116.51.17.201
180.87.108.162
180.87.107.224
63.243.180.64
209.58.82.128
209.58.82.130
?
120.29.211.2
?
66.198.101.133
?
63.243.128.166
63.243.128.26
209.58.18.65
209.58.60.114
x.x.1.1
x.x.1.38
?
x.x.1.38

Hop Count: 29
```

x.x.1.46

2	2	8	1	28
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Tue Apr 16 16:29:55 2024

End time: Tue Apr 16 16:48:44 2024

Host Information

IP: x.x.1.46

OS: Microsoft Windows Server 2008 R2

Vulnerabilities

125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) -

Synopsis

The remote host is affected by a remote code execution vulnerability.

Description

The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2019/05/22, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

34460 - Unsupported Web Server Detection -

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Risk Factor

High

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Plugin Information

Published: 2008/10/21, Modified: 2023/02/10

Plugin Output

tcp/80/www

```
Product : Microsoft IIS 7.5
Server response header : Microsoft-IIS/7.5
Support ended : 2020-01-14
Supported versions : Microsoft IIS 8.5 / 8.0
Additional information : http://www.Soundview Security.org/u?d8353958
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm -

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Soundview Security CA database (known_CA.inc) have been ignored.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

Plugin Information

Published: 2009/01/05, Modified: 2023/12/15

Plugin Output

tcp/3389/msrdp

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

Subject : CN=Mega_Wowza
Signature Algorithm : SHA-1 With RSA Encryption
Valid From : Dec 11 06:00:21 2023 GMT
Valid To : Jun 11 06:00:21 2024 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIC7DCCAdSgAwIBAgIQTRZL195gnLlP0w3a53c8UzANBgkqhkiG9w0BAQUFADAfMR0wGwYDVQQDHhQATQBlAGcAYQBfAFcAbwB3AHoAYTAeFw0yMzEyMTEwN
jAwMjFaFw0yNDA2MTEwNjAwMjFaMB8xHTAbBgNVBAMeFABNAGUAZwBhAF8AVwBvAHcAegBhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApHU328
FUuIix3l66UIw1ysDpgr8ldsgIsjX9oWc5ZZPHLm9uuXfVUzQA+D+R2sYPkii7rQv8I0bvaJFnPHR2C2W1qJvuFI76LD0/CI9Bb9osYvqXbOVHEFebaOP3T5O
8jyesM5Vmf96uN2zFGv/i2TmjIzIL93r3LZW5+7ZrGqt9i/dRWLNV5xtBOrqU4AmC5RNf+/c+XC9zUYj570soTVLarOGwwMsvBqOEKhpjE08L8JipKJbDv//y
VJmdHIe3UDVnSAYpo9SzkVBuZTuWvRbwxNPjgZS8TCkD53Fq4ivfVkCyfAI7ktAhGLbElcKWZSu2n2yrZYaEbiAZnIg1awIDAQABoyQwIjATBgNVHSUEDDAKB
ggrBgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQEFBQADggEBACOr0ZLPgNNt58jPfv0I8HaannCMh5Sdqksy4SQEdFT5c0HZL9JzXdBqjLsk85misQ
a/tr+XzRip3Nrz1Y4yLKtxoCCPJp+FInPEuomNVq0ZveyYLkzZiTS6zbGq0RZ03hrFNSq5j8ThnqmvbT+P9kAwWiEgc7isz1QP6Pv17fzYu6SLYzYRGP6/SKP
hBgYwsr1vAzIrusBV/SJE8WcBOqCfes2ldC37Uu6Ay6PBFWk3R/f+zY1OEKhP8Jbce3lXX3xwG17IVCqkSvdr8cUhi0YzQYfXdyQkMJVewKt1JBjtt5EvgXq9
R5ail0qqlJl7Z+BDQdQs76SEqP8iwjhBsJI=
-----END CERTIFICATE-----
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Soundview Security regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1
```

```
The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness -

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a publicly known hard-coded RSA private key. Any attacker in a privileged network location can use the key for this attack.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Plugin Information

Published: 2005/06/01, Modified: 2022/08/24

Plugin Output

tcp/3389/msrdp

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Soundview Security either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/3389/msrdp

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=Mega_Wowza
|-Issuer : CN=Mega_Wowza
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57582 - SSL Self-Signed Certificate -

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/3389/msrdp

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=Mega_Wowza
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/3389/msrdp

```
TLSv1 is enabled and the server supports at least one cipher.
```

157288 - TLS Version 1.1 Protocol Deprecated -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

tcp/3389/msrdp

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only -

Synopsis

The remote Terminal Services doesn't use Network Level Authentication only.

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

Risk Factor

Medium

CVSS v3.0 Base Score

4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N)

Plugin Information

Published: 2012/03/23, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

```
Soundview Security was able to negotiate non-NLA (Network Level Authentication) security.
```

57690 - Terminal Services Encryption Level is Medium or Low -

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Risk Factor

Medium

Plugin Information

Published: 2012/01/25, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

```
The terminal services encryption level is set to :

2. Medium
```

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant -

Synopsis

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Risk Factor

Low

Plugin Information

Published: 2008/02/11, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

```
The terminal services encryption level is set to :

2. Medium (Client Compatible)
```

45590 - Common Platform Enumeration (CPE) -

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Soundview Security scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/04/03

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:microsoft:windows_server_2008:r2 -> Microsoft Windows Server 2008

Following application CPE matched on the remote system :

cpe:/a:microsoft:iis:7.5 -> Microsoft IIS
```

54615 - Device Type -

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 75
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD POST TRACE OPTIONS are allowed on :

/
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Risk Factor

None

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Microsoft-IIS/7.5
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

Content-Type: text/html
Last-Modified: Mon, 15 Jul 2013 20:46:10 GMT
Accept-Ranges: bytes
ETag: "53ac77569c81ce1:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Mon, 16 Apr 2024 11:39:30 GMT
Content-Length: 689

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS7</title>
<style type="text/css">
<!--
body {
color:#000000;
background-color:#B3B3B3;
margin:0;
}

#container {
margin-left:auto;
margin-right:auto;
text-align:center;
}

a img {
border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="welcome.png" alt="IIS7" width="571"
height="411" /></a>
</div>
</body>
</html>
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

```
Port 3389/tcp was found to be open
```

19506 - Soundview Security Scan Information -

Synopsis

This plugin displays information about the Soundview Security scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Soundview Security or Soundview Security Home).
- The version of the Soundview Security Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/03/13

Plugin Output

tcp/0

```
Information about this scan :

Soundview Security version : 10.7.2
Soundview Security build : 20029
Plugin feed version : 202404150829
Scanner edition used : Soundview Security
```

```
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.126
Port scanner(s) : Soundview Security_syn_scanner
Port range : default
Ping RTT : 398.911 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Soundview Security Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/4/15 16:30 West Asia Standard Time
Scan duration : 1111 sec
Scan for malware : no
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2008 R2
Confidence level : 75
Method : HTTP

The remote host is running Microsoft Windows Server 2008 R2
```

66334 - Patch Report -

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/04/09

Plugin Output

tcp/0

```
. You need to take the following action :
[ Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) (125313) ]
+ Action to take : Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.
```

66173 - RDP Screenshot -

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.

While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Risk Factor

None

Plugin Information

Published: 2013/04/22, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

```
It was possible to gather the following screenshot of the remote login screen.
```

10940 - Remote Desktop Protocol Service Detection -

Synopsis

The remote host has an remote desktop protocol service enabled.

Description

The Remote Desktop Protocol allows a user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2023/08/21

Plugin Output

tcp/3389/msrdp

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon -

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/3389/msrdp

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject : CN=Mega_Wowza
|-Not After : Jun 11 06:00:21 2024 GMT
```

42981 - SSL Certificate Expiry - Future Expiry -

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/3389/msrdp

```
The SSL certificate will expire within 60 days, at
Jun 11 06:00:21 2024 GMT :

Subject : CN=Mega_Wowza
Issuer : CN=Mega_Wowza
Not valid before : Dec 11 06:00:21 2023 GMT
Not valid after : Jun 11 06:00:21 2024 GMT
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: Mega_Wowza

Issuer Name:

Common Name: Mega_Wowza

Serial Number: 4D 16 4B D7 DE 60 9C B9 4F D3 0D DA E7 77 3C 53

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Dec 11 06:00:21 2023 GMT
Not Valid After: Jun 11 06:00:21 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 75 37 DB C1 54 B8 88 B1 DE 5E BA 50 8C 35 CA C0 E9 82
BF 25 76 C8 08 B2 35 FD A1 67 39 65 93 C7 2E 6F 6E B9 77 D5
53 34 00 F8 3F 91 DA C6 0F 92 28 BB AD 0B FC 23 46 EF 68 91
67 3C 74 76 0B 65 B5 A8 9B EE 14 8E FA 2C 3D 3F 08 8F 41 6F
DA 2C 62 FA 97 6C E5 47 10 57 9B 68 E3 F7 4F 93 BC 8F 27 AC
33 95 66 7F DE AE 37 6C C5 1A FF E2 D9 39 A3 23 32 0B F7 7A
F7 2D 95 B9 FB B6 6B 1A AB 7D 8B F7 51 58 B3 55 E7 1B 41 3A
BA 94 E0 09 82 E5 13 5F FB F7 3E 5C 2F 73 51 88 F9 EF 4B 28
4D 52 DA AC E1 B0 C0 CB 2F 06 A3 84 2A 1A 63 13 4F 0B F0 98
A9 28 96 C3 BF FF F2 54 99 9D 1C 87 B7 50 35 67 48 06 29 A3
D4 B3 91 50 6E 65 3B 96 BD 16 F0 C4 D3 E3 81 94 BC 4C 29 03
E7 71 6A E2 2B DF 56 40 B2 7C 02 3B 92 D0 21 18 B6 C4 95 C2
96 65 2B B6 9F 6C AB 65 86 84 6E 20 19 9C 88 35 6B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 23 AB D1 92 CF 80 D3 6D E7 C8 CF 7E FD 08 F0 76 9A 9E 70
8C 87 94 9D AA 4B 32 E1 24 04 74 54 F9 73 41 D9 2F D2 73 5D
D0 6A 8C BB 24 F3 99 A2 B1 06 BF B6 BF 97 CD 18 A9 DC DA F3
D5 8E 32 2C AB 71 A0 20 8F 26 9F 85 22 73 C4 BA 89 8D 56 AD
19 BD EC 98 2E 4C D9 89 34 BA CD B1 AA D1 16 74 DE 1A C5 35
2A B9 8F C4 E1 9E A9 AF 6D 3F 8F F6 40 30 5A 21 20 73 B8 AC
CF 54 0F E8 FB F5 ED FC D8 BB A4 8B 63 36 11 18 FE BF 48 A3
E1 06 06 30 B2 BD 6F 03 32 2B BA C0 55 FD 22 44 F1 67 01 3A
A0 9F 7A CD A5 74 2D FB 52 EE 80 CB A3 C1 15 69 37 47 F7 FE
CD 8D 4E 10 A8 4F F0 96 DC 7B 79 57 5F 7C 70 1B 5E C8 54 2A
A4 4A F7 6B F1 C5 21 8B 46 33 41 87 D7 77 24 24 30 95 5E C0
AB 75 24 18 ED B7 91 2F 81 7A BD 47 96 A2 97 4A AA 94 99 7B
67 E0 43 41 D4 2C EF A4 84 A8 FF 22 C2 38 41 B0 92

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment


Fingerprints :

SHA-256 Fingerprint: E8 8B A0 50 BF 77 B3 02 84 9D F6 8C E0 DD 58 F2 69 0D D2 F1
3A 0B 55 66 0C 7A 5C D5 59 8D C3 A1
SHA-1 Fingerprint: CB FF D9 99 19 CB C2 E4 FF A9 9F F0 E0 81 9C 73 6A 84 60 4E
MD5 Fingerprint: 47 A8 3E 6F E2 CE FE 66 A0 65 E9 3F 54 03 44 42


PEM certificate :

-----BEGIN CERTIFICATE-----
```

```
MIIC7DCCAdSgAwIBAgIQTRZL195gnLlP0w3a53c8UzANBgkqhkiG9w0BAQUFADAfMR0wGwYDVQQDHhQATQBlAGcAYQBfAFcAbwB3AHoAYTAeFw0yMzEyMTEwN
jAwMjFaFw0yNDA2MTEwNjAwMjFaMB8xHTAbBgNVBAMeFABNAGUAZwBhAF8AVwBvAHcAegBhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApHU328
FUuIix3l66UIw1ysDpgr8ldsgIsjX9oWc5ZZPHLm9uuXfVUzQA+D+R2sYPkii7rQv8I0bvaJFnPHR2C2W1qJvuFI76LD0/CI9Bb9osYvqXbOVHEFebaOP3T5O
8jyesM5Vmf96uN2zFGv/i2TmjIzIL93r3LZW5+7ZrGqt9i/dRWLNV5xtBOrqU4AmC5RNf+/c+XC9zUYj570soTVLarOGwwMsvBqOEKhpjE08L8JipKJbDv//y
VJmdHIe3UDVnSAYpo9SzkVBuZTuWvRbwxNPjgZS8TCkD53Fq4ivfVkCyfAI7ktAhGLbElcKWZSu2n2yrZYaEbiAZnIg1awIDAQABoyQwIjATBgNVHSUEDDAKB
ggrBgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQEFBQADggEBACOr0ZLPgNNt58jPfv0I8HaannCMh5Sdqksy4SQEdFT5c0HZL9JzXdBqjLsk85misQ
a/tr+XzRip3Nrz1Y4yLKtxoCCPJp+FInPEuomNVq0ZveyYLkzZiTS6zbGq0RZ03hrFNSq5j8ThnqmvbT+P9kAwWiEgc7isz1QP6Pv17fzYu6SLYzYRGP6/SKP
hBgYwsr1vAzIrusBV/SJE8WcBOqCfes2ldC37Uu6Ay6PBFWk3R/f+zY1OEKhP8Jbce3lXX3xwG17IVCqkSvdr8cUhi0YzQYfXdyQkMJVewKt1JBjtt5EvgXq9
R5ail0qqlJl7Z+BDQdQs76SEqP8iwjhBsJI=
-----END CERTIFICATE-----
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256


SSL Version : TLSv11
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1


SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/3389/msrdp

```
Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- -------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

51891 - SSL Session Resume Supported -

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/3389/msrdp

```
This port supports resuming TLSv1 / TLSv1 / TLSv1 sessions.
```

156899 - SSL/TLS Recommended Cipher Suites -

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:
- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:
- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/3389/msrdp

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Soundview Security was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

25220 - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

121010 - TLS Version 1.1 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/3389/msrdp

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection -

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/3389/msrdp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

64814 - Terminal Services Use SSL/TLS -

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Risk Factor

None

Plugin Information

Published: 2013/02/22, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: Mega_Wowza

Issuer Name:

Common Name: Mega_Wowza

Serial Number: 4D 16 4B D7 DE 60 9C B9 4F D3 0D DA E7 77 3C 53

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Dec 11 06:00:21 2023 GMT
Not Valid After: Jun 11 06:00:21 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 75 37 DB C1 54 B8 88 B1 DE 5E BA 50 8C 35 CA C0 E9 82
BF 25 76 C8 08 B2 35 FD A1 67 39 65 93 C7 2E 6F 6E B9 77 D5
53 34 00 F8 3F 91 DA C6 0F 92 28 BB AD 0B FC 23 46 EF 68 91
67 3C 74 76 0B 65 B5 A8 9B EE 14 8E FA 2C 3D 3F 08 8F 41 6F
DA 2C 62 FA 97 6C E5 47 10 57 9B 68 E3 F7 4F 93 BC 8F 27 AC
33 95 66 7F DE AE 37 6C C5 1A FF E2 D9 39 A3 23 32 0B F7 7A
F7 2D 95 B9 FB B6 6B 1A AB 7D 8B F7 51 58 B3 55 E7 1B 41 3A
BA 94 E0 09 82 E5 13 5F FB F7 3E 5C 2F 73 51 88 F9 EF 4B 28
4D 52 DA AC E1 B0 C0 CB 2F 06 A3 84 2A 1A 63 13 4F 0B F0 98
A9 28 96 C3 BF FF F2 54 99 9D 1C 87 B7 50 35 67 48 06 29 A3
D4 B3 91 50 6E 65 3B 96 BD 16 F0 C4 D3 E3 81 94 BC 4C 29 03
E7 71 6A E2 2B DF 56 40 B2 7C 02 3B 92 D0 21 18 B6 C4 95 C2
96 65 2B B6 9F 6C AB 65 86 84 6E 20 19 9C 88 35 6B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 23 AB D1 92 CF 80 D3 6D E7 C8 CF 7E FD 08 F0 76 9A 9E 70
8C 87 94 9D AA 4B 32 E1 24 04 74 54 F9 73 41 D9 2F D2 73 5D
D0 6A 8C BB 24 F3 99 A2 B1 06 BF B6 BF 97 CD 18 A9 DC DA F3
D5 8E 32 2C AB 71 A0 20 8F 26 9F 85 22 73 C4 BA 89 8D 56 AD
19 BD EC 98 2E 4C D9 89 34 BA CD B1 AA D1 16 74 DE 1A C5 35
2A B9 8F C4 E1 9E A9 AF 6D 3F 8F F6 40 30 5A 21 20 73 B8 AC
CF 54 0F E8 FB F5 ED FC D8 BB A4 8B 63 36 11 18 FE BF 48 A3
E1 06 06 30 B2 BD 6F 03 32 2B BA C0 55 FD 22 44 F1 67 01 3A
A0 9F 7A CD A5 74 2D FB 52 EE 80 CB A3 C1 15 69 37 47 F7 FE
CD 8D 4E 10 A8 4F F0 96 DC 7B 79 57 5F 7C 70 1B 5E C8 54 2A
A4 4A F7 6B F1 C5 21 8B 46 33 41 87 D7 77 24 24 30 95 5E C0
AB 75 24 18 ED B7 91 2F 81 7A BD 47 96 A2 97 4A AA 94 99 7B
67 E0 43 41 D4 2C EF A4 84 A8 FF 22 C2 38 41 B0 92

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment
```

10287 - Traceroute Information -

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.126 to x.x.1.46 :
192.168.0.126
192.168.0.234
39.37.128.1
10.253.9.42
10.253.8.100
10.253.4.16
10.253.4.2
116.51.17.201
?
63.243.180.64
?
180.87.181.25
?
66.198.101.133
?
63.243.128.26
209.58.18.65
209.58.60.114
x.x.1.1
x.x.1.46
?
x.x.1.46

Hop Count: 26
```

11422 - Web Server Unconfigured - Default Install Page Present -

Synopsis

The remote web server is not configured or is improperly configured.

Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2018/08/15

Plugin Output

tcp/80/www

```
The default welcome page is from IIS.
```

x.x.1.79

1	2	13	2	43
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Tue Apr 16 16:29:55 2024

End time: Tue Apr 16 17:01:54 2024

Host Information

IP: x.x.1.79

OS: Microsoft Windows

Vulnerabilities

20007 - SSL Version 2 and 3 Protocol Detection -

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/443/www

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA ECDH RSA AES-CBC(256) SHA1
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
RC4-MD5 RSA RSA RC4(128) MD5
RC4-SHA RSA RSA RC4(128) SHA1
ECDHE-RSA-AES128-SHA256 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Soundview Security regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Soundview Security regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
```

```
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness -

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a publicly known hard-coded RSA private key. Any attacker in a privileged network location can use the key for this attack.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Plugin Information

Published: 2005/06/01, Modified: 2022/08/24

Plugin Output

tcp/3389/msrdp

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Soundview Security either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/443/www

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject : C=US/ST=New York/L=Long Island City/O=Titan Television, LLC/CN=*.GreekEliteTV.com
|-Not After : Jun 26 23:59:59 2023 GMT
```

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Soundview Security either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/3389/msrdp

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=IPTV2
|-Issuer : CN=IPTV2
```

15901 - SSL Certificate Expiry -

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
The SSL certificate has already expired :

Subject : C=US, ST=New York, L=Long Island City, O=Titan Television, LLC, CN=*.GreekEliteTV.com
Issuer : C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
Not valid before : Jul 20 00:00:00 2022 GMT
Not valid after : Jun 26 23:59:59 2023 GMT
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- -------------------- ---
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- -------------------- ---
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57582 - SSL Self-Signed Certificate -

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/3389/msrdp

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=IPTV2
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/443/www

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/3389/msrdp

```
TLSv1 is enabled and the server supports at least one cipher.
```

157288 - TLS Version 1.1 Protocol Deprecated -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

tcp/443/www

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

157288 - TLS Version 1.1 Protocol Deprecated -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

tcp/3389/msrdp

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only -

Synopsis

The remote Terminal Services doesn't use Network Level Authentication only.

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

Risk Factor

Medium

CVSS v3.0 Base Score

4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N)

Plugin Information

Published: 2012/03/23, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

```
Soundview Security was able to negotiate non-NLA (Network Level Authentication) security.
```

57690 - Terminal Services Encryption Level is Medium or Low -

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Risk Factor

Medium

Plugin Information

Published: 2012/01/25, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

```
The terminal services encryption level is set to :

2. Medium
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) -

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Risk Factor

Medium

CVSS v3.0 Base Score

3.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N)

Plugin Information

Published: 2014/10/15, Modified: 2023/06/23

Plugin Output

tcp/443/www

```
Soundview Security determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant -

Synopsis

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Risk Factor

Low

Plugin Information

Published: 2008/02/11, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

```
The terminal services encryption level is set to :

2. Medium (Client Compatible)
```

46180 - Additional DNS Hostnames -

Synopsis

Soundview Security has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Soundview Security has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
- greekelitetv.com
```

45590 - Common Platform Enumeration (CPE) -

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Soundview Security scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/04/03

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:microsoft:windows -> Microsoft Windows
```

54615 - Device Type -

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 70
```

84502 - HSTS Missing From HTTPS Server -

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Risk Factor

None

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Risk Factor

None

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 16 Apr 2024 11:29:59 GMT
Connection: close
Content-Length: 315

Response Body :
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 16 Apr 2024 11:30:07 GMT
Connection: close
Content-Length: 315

Response Body :
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/443/www

```
Port 443/tcp was found to be open
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

```
Port 3389/tcp was found to be open
```

19506 - Soundview Security Scan Information -

Synopsis

This plugin displays information about the Soundview Security scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Soundview Security or Soundview Security Home).
- The version of the Soundview Security Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/03/13

Plugin Output

tcp/0

```
Information about this scan :

Soundview Security version : 10.7.2
Soundview Security build : 20029
Plugin feed version : 202404150829
Scanner edition used : Soundview Security
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.126
Port scanner(s) : Soundview Security_syn_scanner
Port range : default
Ping RTT : 382.912 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Soundview Security Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/4/15 16:30 West Asia Standard Time
Scan duration : 1900 sec
Scan for malware : no
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows
Confidence level : 70
Method : HTTP


The remote host is running Microsoft Windows
```

66173 - RDP Screenshot -

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.

While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Risk Factor

None

Plugin Information

Published: 2013/04/22, Modified: 2024/03/19

Plugin Output

tcp/3389/msrdp

```
It was possible to gather the following screenshot of the remote login screen.
```

10940 - Remote Desktop Protocol Service Detection -

Synopsis

The remote host has an remote desktop protocol service enabled.

Description

The Remote Desktop Protocol allows a user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2023/08/21

Plugin Output

tcp/3389/msrdp

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/443/www

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon -

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/3389/msrdp

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject : CN=IPTV2
|-Not After : May 27 18:00:00 2024 GMT
```

42981 - SSL Certificate Expiry - Future Expiry -

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/3389/msrdp

```
The SSL certificate will expire within 60 days, at
May 27 18:00:00 2024 GMT :

Subject : CN=IPTV2
Issuer : CN=IPTV2
```

```
Not valid before : Nov 26 18:00:00 2023 GMT
Not valid after : May 27 18:00:00 2024 GMT
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Subject Name:

Country: US
State/Province: New York
Locality: Long Island City
Organization: Titan Television, LLC
Common Name: *.GreekEliteTV.com

Issuer Name:

Country: US
Organization: DigiCert Inc
Common Name: DigiCert TLS RSA SHA256 2020 CA1

Serial Number: 0A 8E A8 4B DE 8C A6 FE 15 E8 76 A5 01 35 0F 0A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 20 00:00:00 2022 GMT
Not Valid After: Jun 26 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E2 6A 41 C0 46 7F 93 27 9F D7 AF 7D A9 F8 DC 52 B1 3C 76
58 94 F8 74 20 FA 16 1B 90 35 77 BC C5 0D 5E 10 86 93 DF D6
69 F1 36 C8 8F 44 2A CA 98 94 D6 AC 5A 43 06 33 43 B5 EA FE
EA B4 C6 CF 15 93 4E C5 30 37 F5 0A A1 B4 C6 4C 94 96 8D 74
10 69 89 6D 86 5B E2 17 60 0F B2 9A D6 73 1D 4E AC 26 17 E3
47 4B 60 1D 3B E6 57 46 69 9C 9B 3D 80 07 75 73 BB 27 71 1B
3D D3 E2 45 9A E0 D4 28 E9 38 27 68 19 71 41 56 69 31 1C 1F
85 18 16 88 86 90 FE 79 58 99 B3 A7 E2 3D FE D4 4E A7 09 6D
EB 55 31 4B BB A2 6A 37 AE 3E 27 74 19 CD 43 D6 9D 75 13 45
C3 92 84 7C C5 9D A2 50 5E BC C4 6C 50 15 3C 09 53 6E E9 6B
D2 F0 34 A0 6B 64 05 BD AF A1 9B 88 15 F2 BA 54 0A 5D 5F 3E
14 1E B9 8B 2B 09 33 70 27 EE BF DE E3 48 39 C4 C4 3F 16 DB
B9 C4 3F 79 4A 63 93 E2 4E F2 8B DA 6E D8 8B 9E 8D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 68 2A 14 C6 F9 4D 4A 59 65 49 31 1F D8 81 33 DC 0C D2 C6
B1 F3 06 CF 7C DB 55 48 92 75 ED E5 49 AD 5C 76 A0 4C 75 CE
BD 15 94 08 DD D0 CF 2A 73 4B DE A8 02 BF 03 E0 04 05 52 4B
82 69 0F 78 62 1E CB F1 A9 DC 09 43 2D DF 00 67 5B 60 08 B2
CB CC 12 DB AE DF 82 C7 3D 8E C1 80 97 ED CF E7 EC 68 10 B7
8F 28 DB D1 A1 CA 27 BE 9C 51 D6 37 47 E9 CC A4 99 04 62 95
16 16 71 1F E6 F5 7C 42 5D E6 0F 05 9D B5 0F 96 3D 56 08 91
A9 6F E3 DF 3B E5 1D 3F 93 BE BC 0C 83 71 AA 7E AF EA C0 F5
3D B0 60 F4 77 0C 45 0E E3 FA 88 0B 59 EA F0 6A A1 3E 4D 28
0D 7E 04 4A F6 F3 45 BC 9E 68 5D 4B 1D 08 9E B5 F3 F9 F3 65
C8 E1 31 BA 40 EC 89 9E 32 CF A4 D6 85 AC E3 A7 32 36 96 43
E4 C6 72 98 80 63 91 3A 6F D7 E8 40 62 AE 1E 93 00 15 D9 89
70 12 43 7C 6D 78 3B D0 4D E6 34 43 76 28 01 5F 09

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: B7 6B A2 EA A8 AA 84 8C 79 EA B4 DA 0F 98 B2 C5 95 76 B9 F4


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 26 F1 BF E0 22 FD FA A5 AC 17 92 27 74 97 D7 45 6C C2 A1 63
```

Extension: Subject Alternative Name (2.5.29.17)
Critical: 0
DNS: *.GreekEliteTV.com
DNS: GreekEliteTV.com

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Key Encipherment

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)

Extension: CRL Distribution Points (2.5.29.31)
Critical: 0
URI: http://crl3.digicert.com/DigiCertTLSRSASHA2562020CA1-2.crl
URI: http://crl4.digicert.com/DigiCertTLSRSASHA2562020CA1-2.crl

Extension: Policies (2.5.29.32)
Critical: 0
Policy ID #1: 2.23.140.1.2.2
Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI: http://www.digicert.com/CPS

Extension: Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical: 0
Method#1: Online Certificate Status Protocol
URI: http://ocsp.digicert.com
Method#2: Certificate Authority Issuers
URI: http://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1.crt

Extension: Basic Constraints (2.5.29.19)
Critical: 0

Extension: 1.3.6.1.4.1.11129.2.4.2
Critical: 0
Data: 04 82 01 6A 01 68 00 76 00 E8 3E D0 DA 3E F5 06 35 32 E7 57
28 BC 89 6B C9 03 D3 CB D1 11 6B EC EB 69 E1 77 7D 6D 06 BD
6E 00 00 01 82 1C 2F 39 8D 00 00 04 03 00 47 30 45 02 21 00
EC F8 DA 3B 1D 9C F7 EE 5C 3C 66 A6 2E B8 DA 4D 01 9E 8B D6
B8 29 8C 27 4B 93 45 E8 AF 3D 34 7C 02 20 15 36 DF C3 F9 62
32 9F ED E7 90 6A FB C3 64 EF 04 E4 4D D0 4A FC 36 B8 91 F2
DE 33 0A 84 36 64 00 76 00 35 CF 19 1B BF B1 6C 57 BF 0F AD
4C 6D 42 CB BB B6 27 20 26 51 EA 3F E1 2A EF A8 03 C3 3B D6
4C 00 00 01 82 1C 2F 39 99 00 00 04 03 00 47 30 45 02 21 00
83 16 AE 55 7D 12 88 57 C5 67 18 DE 91 92 23 AF AA 23 5C 02
0F 5F 95 8A 79 BA 50 A2 06 3A 34 80 02 20 3D 51 1B 58 98 27
B6 B7 1D 1A 8C B2 54 9E 76 A2 98 45 96 85 FA 08 46 D6 BC A7
B8 52 41 89 2F 90 00 76 00 B3 73 77 07 E1 84 50 F8 63 86 D6
05 A9 DC 11 09 4A 79 2D B1 67 0C 0B 87 DC F0 03 0E 79 36 A5
9A 00 00 01 82 1C 2F 39 C3 00 00 04 03 00 47 30 45 02 21 00
9A 2A 59 05 DA 94 0C 64 AC 26 57 6D 8A 86 AB 65 01 86 71 A7
ED 7B 56 1C D7 83 1D 8F CA 67 CA C1 02 20 00 E2 1E EF 6D EB
31 75 24 07 C4 CD 0E 00 0D AF 6E DC F1 A2 1B 2B 77 3D 66 16
AB 74 A7 1E 16 EC

Fingerprints :

SHA-256 Fingerprint: C7 40 52 82 85 27 E0 E2 63 C9 A2 CA 6D 68 E3 D0 D1 E6 A6 1F
00 DF B2 7C 3C 0B FE 71 60 9E 8C 3D
SHA-1 Fingerprint: C8 AE 43 39 93 6C D2 7E 7B BB F4 96 3F A1 BC 88 8C 58 85 B3
MD5 Fingerprint: 2D 4B C8 B0 D7 4E 84 29 32 83 FB CD 41 2B 21 F0

PEM certificate :

-----BEGIN CERTIFICATE-----
MIIG1TCCBb2gAwIBAgIQCo6oS96Mpv4V6HalATUPCjANBgkqhkiG9w0BAQsFADBPMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDV
QQDEyBEaWdpQ2VydCBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTAeFw0yMjA3MjAwMDAwMDBaFw0yMzA2MjYyMzU5NTlaMHgxCzAJBgNVBAYTAlVTMREwDwYDVQ
QIEwhOZXcgWW9yazEZMBcGA1UEBxMQTG9uZyBJc2xhbmQgQ2l0eTEeMBwGA1UEChMVVGl0YW4gVGVsZXZpc2lvbiwgTExDMRswGQYDVQQDDBIqLkdyZWVrRWx
pdGVUVi5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDiakHARn+TJ5/Xr32p+NxSsTx2WJT4dCD6FhuQNXe8xQ1eEIaT39Zp8TbIj0QqypiU
1qxaQwYzQ7Xq/uq0xs8Vk07FMDf1CqG0xkyUlo10EGmJbYZb4hdgD7Ka1nMdTqwmF+NHS2AdO+ZXRmmcmz2AB3Vzuydx Gz3T4kWa4NQo6TgnaBlxQVZpMRwfh
RgWiIaQ/nlYmbOn4j3+1E6nCW3rVTFLu6JqN64+J3QZzUPWnXUTRcOShHzFnaJQXrzEbFAVPAlTbulr0vA0oGtkBb2voZuIFfK6VApdXz4UHrmLKwkzcCfuv9
7jSDnExD8W27nEP3lKY5PiTvKL2m7Yi56NAgMBAAGjggOCMIIDfjAfBgNVHSMEGDAWgBS3a6LqqKqEjHnqtNoPmLLFlXa59DAdBgNVHQ4EFgQUJvG/4CL9+qW
sF5IndJfXRWzCoWMwLwYDVR0RBCgwJoISKi5HcmVla0VsaXRlVFYuY29tghBHcmVla0VsaXRlVFYuY29tMA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggr
BgEFBQcDAQYIKwYBBQUHAwIwgY8GA1UdHwSBhzCBhDBAoD6gPIY6aHR0cDovL2NybDMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VExTUlNBU0hBMjU2MjAyMENBM
S0yLmNybDBAoD6gPIY6aHR0cDovL2NybDQuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VExTUlNBU0hBMjU2MjAyMENBMS0yLmNybDA+BgNVHSAENzA1MDMGBmeBDA
ECAjApMCcGCCsGAQUFBwIBFhtodHRwOi8vd3d3LmRpZ2ljZXJ0LmNvbS9DUFMwfQYIKwYBBQUHAQEEcTBvMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWd
pY2VydC5jb20wRwYIKwYBBQUHMAKGO2h0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFRMU1JTQVNIQTI1NjIwMjBDQTEuY3J0MAkGA1UdEwQC
MAAwggF+BgorBgEEAdZ5AgQCBIIBbgSCAWoBaAB2AOg+0No+9QY1MudXKLyJa8kD08vREWvs62nhd31tBr1uAAABghwvOY0AAAQDAEcwRQIhAOz42jsdnPfuX
Dxmpi642k0BnovWuCmMJ0uTReivPTR8AiAVNt/D+WIyn+3nkGr7w2TvBORN0Er8NriR8t4zCoQ2ZAB2ADXPGRu/sWxXvw+tTG1Cy7u2JyAmUeo/4SrvqAPDO9
ZMAAABghwvOZkAAAQDAEcwRQIhAIMWrlV9EohXxWcY3pGSI6+qI1wCD1+Vinm6UKIGOjSAAiA9URtYmCe2tx0ajLJUnnaimEWWhfoIRta8p7hSQYkvkAB2ALN
zdwfhhFD4Y4bWBancEQlKeS2xZwwLh9zwAw55NqWaAAABghwvOcMAAAQDAEcwRQIhAJoqWQXalAxkrCZXbYqGq2UBhnGn7XtWHNeDHY/KZ8rBAiAA4h7vbesx
dSQHxM0OAA2vbtzxohsrdz1mFqt0px4W7DANBgkqhkiG9w0BAQsFAAOCAQEAaCoUxvlNSlllSTEf2IEz3AzSxrHzBs9821VIknXt5UmtXHagTHXOvRWUCN3Qz
ypzS96oAr8D4AQFUkuCaQ94Yh7L8ancCUMt3wBnW2AIssvMEtuu34LHPY7BgJftz+fsaBC3jyjb0aHKJ76cUdY3R+nMpJkEYpUWFnEf5vV8Ql3mDwWdtQ+WPV
YIkalv49875R0/k768DINxqn6v6sD1PbBg9HcMRQ7j+ogLWerwaqE+TSgNfgRK9vNFvJ5oXUsdCJ618/nzZcjhMbpA7ImeMs+k1oWs46cyNpZD5MZymIBjkTp

```
v1+hAYq4ekwAV2YlwEkN8bXg70E3mNEN2KAFfCQ==
-----END CERTIFICATE-----
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: IPTV2

Issuer Name:

Common Name: IPTV2

Serial Number: 1F EF 74 17 6B DA F3 AE 40 9D 33 8A 16 6A 8E 0B

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 26 18:00:00 2023 GMT
Not Valid After: May 27 18:00:00 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B4 05 D1 98 4A D4 10 9B B0 69 73 A6 48 08 4D 54 1E 33 FD
2F 63 BC 27 90 08 F1 E7 E2 F3 CD BF DC 17 21 4D EF ED 8E F9
39 78 B6 71 71 8F EC 8A B2 CC C0 8E 4D 84 C0 5A 56 39 A9 AE
E8 D6 A3 5E 56 93 40 C5 E3 BA AE 05 A1 BD 80 D8 0D DA 95 CD
86 88 2C A1 A5 E6 40 AE A7 B0 03 0C AE D1 BB 19 68 0A 4F 1F
E6 10 55 60 71 DD D5 A0 8B 95 53 40 AD 31 A0 59 BD 6A 38 3D
72 4F 53 27 8D 47 5C 0F 7A 55 8F 4B F2 20 C0 37 D2 21 6D 0E
27 E4 19 8C B2 0F DB B9 7B 5C 2D 69 42 2A E2 93 4C 2C 64 CD
22 7F 34 25 48 12 C0 F7 1E 96 D9 D7 AB CB 38 CB 82 E6 32 E0
28 8A 3C 53 D5 53 CE D0 4B 06 C4 19 39 C1 DF 34 84 EB D9 AF
FB 16 39 7C 45 29 A1 A5 12 2F 09 88 ED 37 62 6D D2 46 12 96
34 DC 08 D2 C7 33 CD 74 64 2E E4 2C 41 70 C4 C1 1A 65 BD 27
0F C6 64 24 90 25 A2 74 A7 40 C4 53 19 B7 0A 4C 4B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 62 D5 7B 40 0E 22 45 AE EC 79 C1 81 83 8C 0E C0 C1 CC FE
25 B6 B6 7E CC FE 32 9D 12 B7 F5 09 62 FB BC C6 F6 87 2C D6
1A B2 EB E7 9B AE 4E 63 11 2B CD 08 06 14 4F 4E 84 F8 A8 A5
67 5F FB 9F BA 92 21 FD 16 6D FA 05 BB 0C 22 54 0E 3F 69 C3
47 88 9E 5A 80 75 B6 DE 9C 58 86 06 4D 38 D5 17 B3 BB B9 97
0D C7 72 64 83 9D 3B 5D FB 70 68 A8 94 84 B9 95 D5 63 1B DB
07 D9 71 77 10 1B 51 C9 D4 AA 5E 99 06 58 21 95 04 C4 1A 00
F6 68 28 10 9F 98 D1 EB 19 80 4B 0A 24 28 35 95 94 9F 64 C2
5F 89 CA 64 39 29 83 18 C5 64 9C 2E DE 94 C0 A9 E1 4D AD 9E
20 31 0E 92 FD 39 E4 AF 7F 3A C0 5D 19 41 56 A2 12 04 66 D6
6E 9A 1E E1 96 0B 2B 6F D2 7B 93 35 B0 15 9B F7 9D 40 2A 34
73 15 FA 65 34 87 E9 A8 26 11 B6 19 DF EC 21 38 CA 03 09 72
09 EB 58 FC 83 96 EF 6A 26 82 72 F8 6F 34 31 29 9F

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment


Fingerprints :

SHA-256 Fingerprint: 52 AA 1B B5 0A 9D 80 70 FC 14 CA AA 54 61 A3 03 6E A1 68 56
97 4E 29 36 1E D0 38 47 F0 63 82 F9
```

```
SHA-1 Fingerprint: A3 EA 78 B5 3B A3 97 BA E4 0B 65 7F CC 1C 1C 75 41 9A DA D8
MD5 Fingerprint: 5A 78 2C C7 71 CC 95 83 91 10 A0 F8 1A 3C 53 0D


PEM certificate :

-----BEGIN CERTIFICATE-----
MIICzjCCAbagAwIBAgIQH+90F2va865AnTOKFmqOCzANBgkqhkiG9w0BAQsFADAQMQ4wDAYDVQQDEwVJUFRWMjAeFw0yMzExMjYxODAwMDBaFw0yNDA1MjcxO
DAwMDBaMBAxDjAMBgNVBAMTBUlQVFYyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtAXRmErUEJuwaXOmSAhNVB4z/S9jvCeQCPHn4vPNv9wXIU
3v7Y75OXi2cXGP7IqyzMCOTYTAWlY5qa7o1qNeVpNAxeO6rgWhvYDYDdqVzYaILKGl5kCup7ADDK7RuxloCk8f5hBVYHHd1aCllVNArTGgWb1qOD1yT1MnjUd
cD3pVj0vyIMA30iFtDifkGYyyD9u5e1wtaUIq4pNMLGTNIn80JUgSwPceltnXq8s4y4LmMuAoijxT1VPO0EsGxBk5wd80hOvZr/sWOXxFKaGlEi8JiO03Ym3S
RhKWNNwI0sczzXRkLuQsQXDEwRplvScPxmQkkCWidKdAxFMZtwpMSwIDAQABoyQwIjATBgNVHSUEDDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIh
vcNAQELBQADggEBAGLVe0AOIkWu7HnBgYOMDsDBzP4ltrZ+zP4ynRK39Qli+7zG9ocs1hqy6+ebrk5jESvNCAYUT06E+KilZ1/7n7qSIf0WbfoFuwwiVA4/ac
NHiJ5agHW23pxYhgZNONUXs7u5lw3HcmSDnTtd+3BoqJSEuZXVYxvbB9lxdxAbUcnUql6ZBlghlQTEGgD2aCgQn5jR6xmASwokKDWVlJ9kwl+JymQ5KYMYxWS
cLt6UwKnhTa2eIDEOkv055K9/OsBdGUFWohIEZtZumh7hlgsrb9J7kzWwFZv3nUAqNHMV+mU0h+moJhG2Gd/sITjKAwlyCetY/IOW72omgnL4bzQxKZ8=
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA) -

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

Risk Factor

None

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

tcp/443/www

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA
Signature Algorithm : SHA-1 With RSA Encryption
Valid From : Nov 10 00:00:00 2006 GMT
Valid To : Nov 10 00:00:00 2031 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBhMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDV
QQLExB3d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCz
AJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5jb20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb29
0IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsBCSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJ
zs4bg7/fzTtxRuLWZscFs3YnFo97nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt43C/dxC//AH2hdmoRBBYMql1GNXRo
r5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7PT19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4gdW7jVg/tRvoSSiicNoxBN
33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbRTLtm8KPiGxvDl7I
90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUwDQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/EsrhMAtudXH
/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJFP
nlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0lsYSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30
d8tbQkCAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
```

```
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/443/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256


SSL Version : TLSv11
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1


SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)
```

```
Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1


SSL Version : SSLv3
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
```

```
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256


SSL Version : TLSv11
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1


SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443/www

```
Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
```

```
The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/3389/msrdp

```
Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

94761 - SSL Root Certification Authority Certificate Information -

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
The following root Certification Authority certificate was found :

|-Subject : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA
```

```
|-Issuer : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA
|-Valid From : Nov 10 00:00:00 2006 GMT
|-Valid To : Nov 10 00:00:00 2031 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

51891 - SSL Session Resume Supported -

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/443/www

```
This port supports resuming SSLv3 / TLSv1 / TLSv1 / TLSv1 sessions.
```

51891 - SSL Session Resume Supported -

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/3389/msrdp

```
This port supports resuming TLSv1 / TLSv1 / TLSv1 sessions.
```

156899 - SSL/TLS Recommended Cipher Suites -

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:
- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:
- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/443/www

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

156899 - SSL/TLS Recommended Cipher Suites -

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:
- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:
- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/3389/msrdp

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Soundview Security was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Soundview Security was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/443/www

```
A TLSv1 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.
```

25220 - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

121010 - TLS Version 1.1 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/443/www

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/3389/msrdp

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection -

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection -

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/3389/msrdp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

64814 - Terminal Services Use SSL/TLS -

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Risk Factor

None

Plugin Information

Published: 2013/02/22, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: IPTV2

Issuer Name:

Common Name: IPTV2

Serial Number: 1F EF 74 17 6B DA F3 AE 40 9D 33 8A 16 6A 8E 0B

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 26 18:00:00 2023 GMT
Not Valid After: May 27 18:00:00 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B4 05 D1 98 4A D4 10 9B B0 69 73 A6 48 08 4D 54 1E 33 FD
2F 63 BC 27 90 08 F1 E7 E2 F3 CD BF DC 17 21 4D EF ED 8E F9
39 78 B6 71 71 8F EC 8A B2 CC C0 8E 4D 84 C0 5A 56 39 A9 AE
E8 D6 A3 5E 56 93 40 C5 E3 BA AE 05 A1 BD 80 D8 0D DA 95 CD
86 88 2C A1 A5 E6 40 AE A7 B0 03 0C AE D1 BB 19 68 0A 4F 1F
E6 10 55 60 71 DD D5 A0 8B 95 53 40 AD 31 A0 59 BD 6A 38 3D
72 4F 53 27 8D 47 5C 0F 7A 55 8F 4B F2 20 C0 37 D2 21 6D 0E
27 E4 19 8C B2 0F DB B9 7B 5C 2D 69 42 2A E2 93 4C 2C 64 CD
22 7F 34 25 48 12 C0 F7 1E 96 D9 D7 AB CB 38 CB 82 E6 32 E0
28 8A 3C 53 D5 53 CE D0 4B 06 C4 19 39 C1 DF 34 84 EB D9 AF
FB 16 39 7C 45 29 A1 A5 12 2F 09 88 ED 37 62 6D D2 46 12 96
34 DC 08 D2 C7 33 CD 74 64 2E E4 2C 41 70 C4 C1 1A 65 BD 27
0F C6 64 24 90 25 A2 74 A7 40 C4 53 19 B7 0A 4C 4B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 62 D5 7B 40 0E 22 45 AE EC 79 C1 81 83 8C 0E C0 C1 CC FE
25 B6 B6 7E CC FE 32 9D 12 B7 F5 09 62 FB BC C6 F6 87 2C D6
1A B2 EB E7 9B AE 4E 63 11 2B CD 08 06 14 4F 4E 84 F8 A8 A5
67 5F FB 9F BA 92 21 FD 16 6D FA 05 BB 0C 22 54 0E 3F 69 C3
47 88 9E 5A 80 75 B6 DE 9C 58 86 06 4D 38 D5 17 B3 BB B9 97
0D C7 72 64 83 9D 3B 5D FB 70 68 A8 94 84 B9 95 D5 63 1B DB
07 D9 71 77 10 1B 51 C9 D4 AA 5E 99 06 58 21 95 04 C4 1A 00
F6 68 28 10 9F 98 D1 EB 19 80 4B 0A 24 28 35 95 94 9F 64 C2
5F 89 CA 64 39 29 83 18 C5 64 9C 2E DE 94 C0 A9 E1 4D AD 9E
20 31 0E 92 FD 39 E4 AF 7F 3A C0 5D 19 41 56 A2 12 04 66 D6
6E 9A 1E E1 96 0B 2B 6F D2 7B 93 35 B0 15 9B F7 9D 40 2A 34
73 15 FA 65 34 87 E9 A8 26 11 B6 19 DF EC 21 38 CA 03 09 72
09 EB 58 FC 83 96 EF 6A 26 82 72 F8 6F 34 31 29 9F

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment
```

10287 - Traceroute Information -

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.126 to x.x.1.79 :
192.168.0.126
192.168.0.234
39.37.128.1
10.253.9.38
10.253.8.12
10.253.4.16
10.253.4.2
116.51.17.201
180.87.108.162
180.87.107.224
63.243.180.64
209.58.82.128
?
120.29.211.2
209.58.86.200
?
66.198.101.131
63.243.128.30
63.243.128.26
209.58.18.65
209.58.60.114
x.x.1.1
x.x.1.79
?
x.x.1.79

Hop Count: 27
```

x.x.1.80

11	10	9	0	17
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Tue Apr 16 16:29:55 2024
End time:	Tue Apr 16 16:46:37 2024

Host Information

IP:	x.x.1.80
OS:	Microsoft Windows Embedded Standard 7

Vulnerabilities

100995 - Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.33-dev or 2.4.x prior to 2.4.26. It is, therefore, affected by the following vulnerabilities :

- An authentication bypass vulnerability exists due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An

unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167)

- A NULL pointer dereference flaw exists due to third-party module calls to the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169)

- A NULL pointer dereference flaw exists in mod_http2 that is triggered when handling a specially crafted HTTP/2 request. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. Note that this vulnerability does not affect 2.2.x.
(CVE-2017-7659)

- An out-of-bounds read error exists in the ap_find_token() function due to improper handling of header sequences. An unauthenticated, remote attacker can exploit this, via a specially crafted header sequence, to cause a denial of service condition.
(CVE-2017-7668)

- An out-of-bounds read error exists in mod_mime due to improper handling of Content-Type response headers. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type response header, to cause a denial of service condition or the disclosure of sensitive information. (CVE-2017-7679)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2017/06/22, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Installed version : 2.2.22
Fixed version : 2.2.33
```

101787 - Apache 2.2.x < 2.2.34 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.34. It is, therefore, affected by the following vulnerabilities :

- An authentication bypass vulnerability exists in httpd due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167)

- A denial of service vulnerability exists in httpd due to a NULL pointer dereference flaw that is triggered when a third-party module calls the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169)

- A denial of service vulnerability exists in httpd due to an out-of-bounds read error in the ap_find_token() function that is triggered when handling a specially crafted request header sequence. An unauthenticated, remote attacker can exploit this to crash the service or force ap_find_token() to return an incorrect value. (CVE-2017-7668)

- A denial of service vulnerability exists in httpd due to an out-of-bounds read error in the mod_mime that is triggered when handling a specially crafted Content-Type response header. An unauthenticated, remote attacker can exploit this to disclose sensitive information or cause a denial of service condition. (CVE-2017-7679)

- A denial of service vulnerability exists in httpd due to a failure to initialize or reset the value placeholder in [Proxy-]Authorization headers of type 'Digest' before or between successive key=value assignments by mod_auth_digest. An unauthenticated, remote attacker can exploit this, by providing an initial key with no '=' assignment, to disclose sensitive information or cause a denial of service condition. (CVE-2017-9788)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2017/07/18, Modified: 2018/09/17

Plugin Output

tcp/80/www

```
Source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 2.2.22
Fixed version : 2.2.34
```

158900 - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.

- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)

- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)

- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)

- Read/write beyond bounds in mod_sed: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Acknowledgements: Ronald Crane (Zippenhop LLC) (CVE-2022-23943)

Note that Soundview Security has not tested for this issue but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2022/03/14, Modified: 2023/11/06

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Installed version : 2.2.22
Fixed version : 2.4.53
```

161948 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Possible request smuggling in mod_proxy_ajp: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions. Acknowledgements: Ricter Z @ 360 Noah Lab (CVE-2022-26377)

- Read beyond bounds in mod_isapi: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the

mod_isapi module. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28330)

- Read beyond bounds via ap_rwrite(): The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28614)

- Read beyond bounds in ap_strcmp_match(): Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28615)

- Denial of service in mod_lua r:parsebody: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-29404)

- Denial of Service mod_sed: If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort. Acknowledgements: This issue was found by Brian Moussalli from the JFrog Security Research team (CVE-2022-30522)

- Information Disclosure in mod_lua with websockets: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-30556)

- X-Forwarded-For dropped by hop-by-hop mechanism in mod_proxy: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application. Acknowledgements: The Apache HTTP Server project would like to thank Gaetan Ferry (Synacktiv) for reporting this issue (CVE-2022-31813)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2022/06/08, Modified: 2023/10/25

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Installed version : 2.2.22
Fixed version : 2.4.54
```

170113 - Apache 2.4.x < 2.4.55 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.55. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.55 advisory.

- A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier. (CVE-2006-20001)

- Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
(CVE-2022-36760)

- Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client. (CVE-2022-37436)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)

Plugin Information

Published: 2023/01/18, Modified: 2023/03/10

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Installed version : 2.2.22
Fixed version : 2.4.55
```

172186 - Apache 2.4.x < 2.4.56 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory.

- HTTP request splitting with mod_rewrite and mod_proxy: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule ^/here/(.*) http://example.com:8080/elsewhere?$1 http://example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Acknowledgements: finder: Lars Krapf of Adobe (CVE-2023-25690)

- Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.
Special characters in the origin response header can truncate/split the response forwarded to the client.
Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2023/03/07, Modified: 2023/10/21

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Installed version : 2.2.22
Fixed version : 2.4.56
```

153583 - Apache < 2.4.49 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog.

- A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. (CVE-2021-40438)

Note that Soundview Security has not tested for this issue but has instead relied only on the application's self-reported version number.

Risk Factor

Medium

CVSS v3.0 Base Score

9.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)

Plugin Information

Published: 2021/09/23, Modified: 2023/04/25

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Installed version : 2.2.22
Fixed version : 2.4.49
```

153584 - Apache < 2.4.49 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.49 changelog.

- ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. (CVE-2021-39275)

- Malformed requests may cause the server to dereference a NULL pointer. (CVE-2021-34798)

Note that Soundview Security has not tested for this issue but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2021/09/23, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Installed version : 2.2.22
Fixed version : 2.4.49
```

171356 - Apache HTTP Server SEoL (2.1.x <= x <= 2.2.x) -

Synopsis

An unsupported version of Apache HTTP Server is installed on the remote host.

Description

According to its version, Apache HTTP Server is between 2.1.x and 2.2.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Plugin Information

Published: 2023/02/10, Modified: 2024/04/02

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Installed version : 2.2.22
Security End of Life : July 10, 2017
Time since Security End of Life (Est.) : >= 6 years
```

60085 - PHP 5.3.x < 5.3.15 Multiple Vulnerabilities -

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.15, and is, therefore, potentially affected by the following vulnerabilities :

- An unspecified overflow vulnerability exists in the function '_php_stream_scandir' in the file 'main/streams/streams.c'. (CVE-2012-2688)

- An unspecified error exists that can allow the 'open_basedir' constraint to be bypassed.
(CVE-2012-3365)

Risk Factor

Critical

Plugin Information

Published: 2012/07/20, Modified: 2022/04/07

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 5.3.13
Fixed version : 5.3.15
```

58987 - PHP Unsupported Version Detection -

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Plugin Information

Published: 2012/05/04, Modified: 2024/03/22

Plugin Output

tcp/80/www

```
Source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
```

```
Installed version : 5.3.13
End of support date : 2014/08/14
Announcement : http://php.net/eol.php
Supported versions : 8.0.x / 8.1.x
```

62101 - Apache 2.2.x < 2.2.23 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.23. It is, therefore, potentially affected by the following vulnerabilities :

- The utility 'apachectl' can receive a zero-length directory name in the LD_LIBRARY_PATH via the 'envvars' file. A local attacker with access to that utility could exploit this to load a malicious Dynamic Shared Object (DSO), leading to arbitrary code execution. (CVE-2012-0883)

- An input validation error exists related to 'mod_negotiation', 'Multiviews' and untrusted uploads that can allow cross-site scripting attacks. (CVE-2012-2687)

Note that Soundview Security has not tested for these flaws but has instead relied on the version in the server's banner.

Risk Factor

Medium

CVSS v3.0 Base Score

7.0 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

Plugin Information

Published: 2012/09/14, Modified: 2018/06/29

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 2.2.22
Fixed version : 2.2.23
```

77531 - Apache 2.2.x < 2.2.28 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.28. It is, therefore, affected by the following vulnerabilities :

- A flaw exists within the 'mod_headers' module which allows a remote attacker to inject arbitrary headers. This is done by placing a header in the trailer portion of data being sent using chunked transfer encoding. (CVE-2013-5704)

- A flaw exists within the 'mod_deflate' module when handling highly compressed bodies. Using a specially crafted request, a remote attacker can exploit this to cause a denial of service by exhausting memory and CPU resources. (CVE-2014-0118)

- The 'mod_status' module contains a race condition that can be triggered when handling the scoreboard. A remote attacker can exploit this to cause a denial of service, execute arbitrary code, or obtain sensitive credential information. (CVE-2014-0226)

- The 'mod_cgid' module lacks a time out mechanism. Using a specially crafted request, a remote attacker can use this flaw to cause a denial of service by causing child processes to linger indefinitely, eventually filling up the scoreboard. (CVE-2014-0231)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

Medium

CVSS v3.0 Base Score

7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

Plugin Information

Published: 2014/09/04, Modified: 2020/04/27

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 2.2.22
Fixed version : 2.2.29
```

183391 - Apache 2.4.x < 2.4.58 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.58 advisory.

- mod_macro buffer over-read: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57. Acknowledgements: finder: David Shoon (github/davidshoon) (CVE-2023-31122)

- Apache HTTP Server: DoS in HTTP/2 with initial windows size 0: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known slow loris attack pattern. This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57. Users are recommended to upgrade to version 2.4.58, which fixes the issue.
Acknowledgements: (CVE-2023-43622)

- Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During normal HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue. Acknowledgements: (CVE-2023-45802)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Plugin Information

Published: 2023/10/19, Modified: 2024/04/11

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Installed version : 2.2.22
Fixed version : 2.4.58
```

192923 - Apache 2.4.x < 2.4.59 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.59. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.59 advisory.

- Apache HTTP Server: HTTP Response Splitting in multiple modules: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack. Users are recommended to upgrade to version 2.4.59, which

fixes this issue. Acknowledgements: (CVE-2024-24795)

- Apache HTTP Server: HTTP/2 DoS by memory exhaustion on endless continuation frames: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion. Acknowledgements: finder: Bartek Nowotarski (https://nowotarski.info/) (CVE-2024-27316)

Note that Soundview Security has not tested for these issues but has instead relied only on the application's self-reported version number.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Plugin Information

Published: 2024/04/04, Modified: 2024/04/12

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Installed version : 2.2.22
Fixed version : 2.4.59
```

59529 - PHP 5.3.x < 5.3.14 Multiple Vulnerabilities -

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.14, and is, therefore, potentially affected the following vulnerabilities :

- An integer overflow error exists in the function 'phar_parse_tarfile' in the file 'ext/phar/tar.c'. This error can lead to a heap-based buffer overflow when handling a maliciously crafted TAR file. Arbitrary code execution is possible due to this error. (CVE-2012-2386)

- A weakness exists in the 'crypt' function related to the DES implementation that can allow brute-force attacks. (CVE-2012-2143)

- Several design errors involving the incorrect parsing of PHP PDO prepared statements could lead to disclosure of sensitive information or denial of service. (CVE-2012-3450)

- A variable initialization error exists in the file 'ext/openssl/openssl.c' that can allow process memory contents to be disclosed when input data is of length zero. (CVE-2012-6113)

Risk Factor

High

Plugin Information

Published: 2012/06/15, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 5.3.13
Fixed version : 5.3.14
```

64992 - PHP 5.3.x < 5.3.22 Multiple Vulnerabilities -

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.22. It is, therefore, potentially affected by the following vulnerabilities :

- An error exists in the file 'ext/soap/soap.c'
related to the 'soap.wsdl_cache_dir' configuration directive and writing cache files that could allow remote 'wsdl' files to be written to arbitrary locations. (CVE-2013-1635)

- An error exists in the file 'ext/soap/php_xml.c'
related to parsing SOAP 'wsdl' files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1643)

Note that this plugin does not attempt to exploit the vulnerabilities but, instead relies only on PHP's self-reported version number.

Risk Factor

High

Plugin Information

Published: 2013/03/04, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 5.3.13
Fixed version : 5.3.22
```

66584 - PHP 5.3.x < 5.3.23 Multiple Vulnerabilities -

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.23. It is, therefore, potentially affected by multiple vulnerabilities:

- An error exists in the file 'ext/soap/soap.c'
related to the 'soap.wsdl_cache_dir' configuration directive and writing cache files that could allow remote 'wsdl' files to be written to arbitrary locations. (CVE-2013-1635)

- An error exists in the file 'ext/soap/php_xml.c'
related to parsing SOAP 'wsdl' files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1643)

- An information disclosure in the file 'ext/soap/php_xml.c' related to parsing SOAP 'wsdl'
files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1824)

Note that this plugin does not attempt to exploit the vulnerability, but instead relies only on PHP's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

Plugin Information

Published: 2013/05/24, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 5.3.13
Fixed version : 5.3.23
```

71426 - PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities -

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.28. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists in the PHP OpenSSL extension's hostname identity check when handling certificates that contain hostnames with NULL bytes. An attacker could potentially exploit this flaw to conduct man-in-the-middle attacks to spoof SSL servers. Note that to exploit this issue, an attacker would need to obtain a carefully-crafted certificate signed by an authority that the client trusts. (CVE-2013-4073, CVE-2013-4248)

- A memory corruption flaw exists in the way the openssl_x509_parse() function of the PHP OpenSSL extension parsed X.509 certificates. A remote attacker could use this flaw to provide a malicious, self-signed certificate or a certificate signed by a trusted authority to a PHP application using the aforementioned function. This could cause the application to crash or possibly allow the attacker to execute arbitrary code with the privileges of the user running the PHP interpreter. (CVE-2013-6420)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

Risk Factor

High

CVSS v3.0 Base Score

7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

Plugin Information

Published: 2013/12/14, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 5.3.13
Fixed version : 5.3.28
```

77285 - PHP 5.3.x < 5.3.29 Multiple Vulnerabilities -

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.29. It is, therefore, affected by the following vulnerabilities :

- A heap-based buffer overflow error exists in the file 'ext/date/lib/parse_iso_intervals.c' related to handling DateInterval objects that allows denial of service attacks. (CVE-2013-6712)

- A boundary checking error exists related to the Fileinfo extension, Composite Document Format (CDF) handling, and the function 'cdf_read_short_sector'. (CVE-2014-0207)

- A flaw exists with the 'cdf_unpack_summary_info()'
function within 'src/cdf.c' where multiple file_printf calls occur when handling specially crafted CDF files.
This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0237)

- A flaw exists with the 'cdf_read_property_info()'
function within 'src/cdf.c' where an infinite loop occurs when handling specially crafted CDF files. This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0238)

- A type-confusion error exists related to the Standard PHP Library (SPL) extension and the function 'unserialize'. (CVE-2014-3515)

- An error exists related to configuration scripts and temporary file handling that could allow insecure file usage. (CVE-2014-3981)

- A heap-based buffer overflow error exists related to the function 'dns_get_record' that could allow execution of arbitrary code. (CVE-2014-4049)

- An out-of-bounds read exists in printf. (Bug #67249)

Note that Soundview Security has not attempted to exploit these issues, but has instead relied only on the application's self-reported version number.

Additionally, note that version 5.3.29 marks the end of support for the PHP 5.3.x branch.

Risk Factor

High

CVSS v3.0 Base Score

7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

Plugin Information

Published: 2014/08/20, Modified: 2022/04/07

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 5.3.13
Fixed version : 5.3.29
```

142591 - PHP < 7.3.24 Multiple Vulnerabilities -

Synopsis

The version of PHP running on the remote web server is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Plugin Information

Published: 2020/11/06, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/ (5.3.13 under Server: Apache/2.2.22 (Win32) PHP/5.3.13)
Installed version : 5.3.13
Fixed version : 7.3.24
```

64912 - Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities -

Synopsis

The remote web server is affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.24. It is, therefore, potentially affected by the following cross-site scripting vulnerabilities :

- Errors exist related to the modules mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp and unescaped hostnames and URIs that could allow cross- site scripting attacks. (CVE-2012-3499)

- An error exists related to the mod_proxy_balancer module's manager interface that could allow cross-site scripting attacks. (CVE-2012-4558)

Note that Soundview Security did not actually test for these issues, but instead has relied on the version in the server's banner.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Plugin Information

Published: 2013/02/27, Modified: 2018/06/29

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 2.2.22
Fixed version : 2.2.24
```

68915 - Apache 2.2.x < 2.2.25 Multiple Vulnerabilities -

Synopsis

The remote web server may be affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists in the 'RewriteLog' function where it fails to sanitize escape sequences from being written to log files, making it potentially vulnerable to arbitrary command execution. (CVE-2013-1862)

- A denial of service vulnerability exists relating to the 'mod_dav' module as it relates to MERGE requests.
(CVE-2013-1896)

Note that Soundview Security did not actually test for these issues, but instead has relied on the version in the server's banner.

Risk Factor

Medium

CVSS v3.0 Base Score

5.6 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)

Plugin Information

Published: 2013/07/16, Modified: 2018/06/29

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 2.2.22
Fixed version : 2.2.25
```

73405 - Apache 2.2.x < 2.2.27 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is a version prior to 2.2.27. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists with the 'mod_dav' module that is caused when tracking the length of CDATA that has leading white space. A remote attacker with a specially crafted DAV WRITE request can cause the service to stop responding.
(CVE-2013-6438)

- A flaw exists in 'mod_log_config' module that is caused when logging a cookie that has an unassigned value. A remote attacker with a specially crafted request can cause the service to crash. (CVE-2014-0098)

Note that Soundview Security did not actually test for these issues, but instead has relied on the version in the server's banner.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Plugin Information

Published: 2014/04/08, Modified: 2018/09/17

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 2.2.22
Fixed version : 2.2.27
```

88098 - Apache Server ETag Header Information Disclosure -

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Plugin Information

Published: 2016/01/22, Modified: 2020/04/27

Plugin Output

tcp/80/www

```
Soundview Security was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

Source : ETag: "100000000edad-1442-4bc6ecdae0180"
Inode number : 60845
File size : 5186 bytes
File modification time : Mar. 30, 2012 at 05:06:30 GMT
```

10756 - Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing -

Synopsis

It is possible to get the list of files present in the remote directory.

Description

It is possible to read a '.DS_Store' file on the remote web server.

This file is created by MacOS X Finder; it is used to remember the icons position on the desktop, among other things, and contains the list of files and directories present in the remote directory.

Note that deleted files may still be present in this .DS_Store file.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Plugin Information

Published: 2001/09/14, Modified: 2023/10/27

Plugin Output

tcp/80/www

```
http://x.x.1.80/.DS_Store
reveals the following entries:
images
banner.swf_content
config.xml
Gallery.html
contact.php
contact.html
```

11213 - HTTP TRACE / TRACK Methods Allowed -

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

Plugin Output

tcp/80/www

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Soundview Security sent the following TRACE request : \n\n------------------------------ snip ---------------------------
---\nTRACE /Soundview Security789109738.html HTTP/1.1
Connection: Close
Host: x.x.1.80
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n\nand received the following response from the remote
server :\n\n------------------------------ snip ------------------------------\nHTTP/1.1 200 OK
Date: Mon, 16 Apr 2024 11:35:14 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.13
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Soundview Security789109738.html HTTP/1.1
Connection: Keep-Alive
Host: x.x.1.80
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n
```

66842 - PHP 5.3.x < 5.3.26 Multiple Vulnerabilities -

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.26. It is, therefore, potentially affected by the following vulnerabilities:

- An error exists in the function 'php_quot_print_encode'
in the file 'ext/standard/quot_print.c' that could allow a heap-based buffer overflow when attempting to parse certain strings (Bug #64879)

- An integer overflow error exists related to the value of 'JEWISH_SDN_MAX' in the file 'ext/calendar/jewish.c'
that could allow denial of service attacks. (Bug #64895)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

Risk Factor

Medium

Plugin Information

Published: 2013/06/07, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 5.3.13
Fixed version : 5.3.26
```

67259 - PHP 5.3.x < 5.3.27 Multiple Vulnerabilities -

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.27. It is, therefore, potentially affected by the following vulnerabilities:

- A buffer overflow error exists in the function '_pdo_pgsql_error'. (Bug #64949)

- A heap corruption error exists in numerous functions in the file 'ext/xml/xml.c'. (CVE-2013-4113 / Bug #65236)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

Risk Factor

Medium

Plugin Information

Published: 2013/07/12, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
Installed version : 5.3.13
Fixed version : 5.3.27
```

152853 - PHP < 7.3.28 Email Header Injection -

Synopsis

The version of PHP running on the remote web server is affected by an email header injection vulnerability.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.28.
It is, therefore affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Plugin Information

Published: 2021/08/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/ (5.3.13 under Server: Apache/2.2.22 (Win32) PHP/5.3.13)
Installed version : 5.3.13
Fixed version : 7.3.28
```

48204 - Apache HTTP Server Version -

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Risk Factor

None

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL : http://x.x.1.80/
Version : 2.2.22
Source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
backported : 0
modules : PHP/5.3.13
os : Win32
```

45590 - Common Platform Enumeration (CPE) -

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Soundview Security scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/04/03

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:microsoft:windows -> Microsoft Windows

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server
cpe:/a:php:php:5.3.13 -> PHP PHP
```

54615 - Device Type -

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : unknown
Confidence level : 56
```

10092 - FTP Server Detection -

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

/
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Risk Factor

None

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.2.22 (Win32) PHP/5.3.13
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Mon, 16 Apr 2024 11:39:22 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.13
Last-Modified: Fri, 30 Mar 2012 05:06:30 GMT
ETag: "100000000edad-1442-4bc6ecdae0180"
Accept-Ranges: bytes
Content-Length: 5186
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Khalsatours</title>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<link href="style.css" rel="stylesheet" type="text/css" />
<script type="text/javascript" src="js/swfobject/swfobject.js"></script>
<script src="Scripts/swfobject_modified.js" type="text/javascript"></script>
<script type="text/javascript">
var flashvars = {};
flashvars.xml = "config.xml";
flashvars.font = "font.swf";
var attributes = {};
attributes.wmode = "transparent";
attributes.id = "slider";
swfobject.embedSWF("cu3er.swf", "cu3er-container", "960", "400", "9", "expressInstall.swf", flashvars, attributes);
</script>
<style type="text/css">
body {
background-image: url(images/Orangetexture_bg.jpg);
background-repeat: no-repeat;
background-color: #f3f3f3;
background-attachment: fixed;
}
body,td,th {
font-size: small;
font-family: "Arial Black", Gadget, sans-serif;
text-align: left;
}
</style>
</head>
<body>
<div class="main">
<div class="blok_header">
<div class="header">
<div class="search">
<div align="right" class="tel">855 - 5KHALSA </div>
<form id="form1" name="form1" method="post" action="">
</form>
</div>
<div class="clr"></div>
<div class="withe_bg">
<div class="logo"> <a href="index copy.html"><img src="images/khalsalogo.jpg" width="395" height="109" alt="logo" /></a>
</div>
<div class="menu">
<ul>
<li><a href="index.html" class="active">Home Page</a></li>
<li><a href="About Us.html"> About us</a></li>
<li><a href="Tours.html">Tours</a></li>
<li></li>
<li><a href="contact.html"> Contact Us</a></li>
</ul>
</div>
<div class="cu3er_resize">
<p align="center" id="FlashID2" title="newbanner" classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" width="935"
height="287">
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" width="935" height="287" title="newbanner">
<param name="movie" value="newbanner.swf" />
<param name="quality" value="high" />
<param name="wmode" value="opaque" />
<param name="swfversion" value="6.0.65.0" />
<!-- This param tag prompts users with Flash Player 6.0 r65 and higher to download the latest version of Flash Player.
Delete it if you don’t want users to see the prompt. -->
<param name="expressinstall" value="Scripts/expressInstall.swf" />
<!-- Next object tag is for non-IE browsers. So hide it from IE using IECC. -->
<!--[if !IE]>-->
<object type="application/x-shockwave-flash" data="newbanner.swf" width="935" height="287">
<!--<![endif]-->
<param name="quality" value="high" />
<param name="wmode" value="opaque" />
<param name="swfversion" value="6.0.65.0" />
<param name="expressinstall" value="Scripts/expressInstall.swf" />
```

```
<!-- The browser displays the following alternative content for users with Flash Player 6.0 and older. -->
<div>
<h4>Content on this page requires a newer version of Adobe Flash Player.</h4>
<p><a href="http://www.adobe.com/go/getflashplayer"><img
src="http://www.adobe.com/images/shared/download_buttons/get_flash_player.gif" alt="Get Adobe Flash player" width="112"
height="33" /></a></p>
</div>
<!--[if !IE]>-->
</object>
<!--<![endif]-->
</object>
</p>
</div>
<div class="clr"></div>
<div class="body">
<h2>For the first time ever, in collaboration with the Pakistan Tourism Authority, we are proud to offer Sikhs throughout
North America the experience of a lifetime -- access to previously closed-off holy historical Gurdwaras in Pakistan.
</h2>
<p align="center"> </p>
<table width="920" height="82">
<tr>
<td>Next Tour: April 7th - April 16th <img src="images/AprilTable.jpg" width="920" height="403" alt="april table" /></td>
</tr>
</table>
<div class="clr"></div>
</div>
<div class="clr"></div>
</div>
<div class="clr"></div>
</div>
</div>
<div class="clr"></div>
</div>
<div class="FBG">
<div class="clr"></div>
</div>
<div class="footer">
<div class="footer_resize"><a href="index copy.html"><img src="images/offwhitekhalsalogo.jpg" width="153" height="45"
alt="offwhitelogo" /></a>
<p class="leftt">© Copyright websitename . All Rights Reserved.</p>
<p class="right"> </p>
<div class="clr"></div>
</div>
<div class="clr"></div>
</div>
<script type="text/javascript">
swfobject.registerObject("FlashID2");
</script>
</body>
</html>
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

11219 - Soundview Security SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

19506 - Soundview Security Scan Information -

Synopsis

This plugin displays information about the Soundview Security scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Soundview Security or Soundview Security Home).
- The version of the Soundview Security Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/03/13

Plugin Output

tcp/0

```
Information about this scan :

Soundview Security version : 10.7.2
Soundview Security build : 20029
Plugin feed version : 202404150829
Scanner edition used : Soundview Security
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.126
Port scanner(s) : Soundview Security_syn_scanner
Port range : default
Ping RTT : 415.968 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
```

```
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Soundview Security Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/4/15 16:30 West Asia Standard Time
Scan duration : 982 sec
Scan for malware : no
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Embedded Standard 7
Confidence level : 56
Method : MLSinFP


The remote host is running Microsoft Windows Embedded Standard 7
```

48243 - PHP Version Detection -

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Soundview Security was able to determine the version of PHP available on the remote web server.

Risk Factor

None

Plugin Information

Published: 2010/08/04, Modified: 2022/10/12

Plugin Output

tcp/80/www

```
Soundview Security was able to identify the following PHP version information :

Version : 5.3.13
Source : Server: Apache/2.2.22 (Win32) PHP/5.3.13
```

66334 - Patch Report -

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/04/09

Plugin Output

tcp/0

```
. You need to take the following 2 actions :

[ Apache 2.4.x < 2.4.59 Multiple Vulnerabilities (192923) ]

+ Action to take : Upgrade to Apache version 2.4.59 or later.

+Impact : Taking this action will resolve 44 different vulnerabilities (CVEs).


[ PHP 5.3.x < 5.3.29 Multiple Vulnerabilities (77285) ]

+ Action to take : Upgrade to PHP version 5.3.29 or later.

+Impact : Taking this action will resolve 15 different vulnerabilities (CVEs).
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Soundview Security was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Soundview Security was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

25220 - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

10287 - Traceroute Information -

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.126 to x.x.1.80 :
192.168.0.126
192.168.0.234
39.37.128.1
10.253.9.42
10.253.8.100
10.253.4.36
10.253.4.24
116.51.17.201
180.87.108.162
180.87.107.224
63.243.180.64
209.58.82.128
?
120.29.211.2
?
63.243.128.166
63.243.128.26
209.58.18.65
209.58.60.114
x.x.1.1
x.x.1.80
?
x.x.1.80

Hop Count: 25
```