Reto_4_exex__Spring_4_CN

Report generated by Nessus™ Thu, 27 Jun 2024 03:16:36 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.0.2.8.....4

Vulnerabilities by Host

10.0.2.8

CRITICAL	HIGH	MEDIUM	LOW	INFO
15	24	33	3	122

Scan Information

Start time: Thu Jun 27 02:44:57 2024
End time: Thu Jun 27 03:16:36 2024

Host Information

Netbios Name: METASPLOITABLE3
IP: 10.0.2.8
MAC Address: 08:00:27:41:0F:1C DA:D6:20:52:41:53 08:00:27:12:95:5B
OS: Microsoft Windows Server 2008 R2 Standard Service Pack 1

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

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.32

https://archive.apache.org/dist/httpd/CHANGES_2.4.26

https://httpd.apache.org/security/vulnerabilities_22.html

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.2.33-dev / 2.4.26 or later.

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)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	99132
BID	99134

BID	99135
BID	99137
BID	99170
CVE	CVE-2017-3167
CVE	CVE-2017-3169
CVE	CVE-2017-7659
CVE	CVE-2017-7668
CVE	CVE-2017-7679

Plugin Information

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

Plugin Output

tcp/8585/www

```
URL              : http://10.0.2.8:8585/
Installed version : 2.2.21
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 Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.34

https://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.34 or later.

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)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	99134
BID	99135
BID	99137
BID	99170
BID	99569
CVE	CVE-2017-3167
CVE	CVE-2017-3169
CVE	CVE-2017-7668
CVE	CVE-2017-7679
CVE	CVE-2017-9788

Plugin Information

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

Plugin Output

tcp/8585/www

```
Source            : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
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 Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.apache.org/dist/httpd/Announcement2.4.html

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.53 or later.

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)

CVSS v3.0 Temporal Score

9.1 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-22719
CVE	CVE-2022-22720
CVE	CVE-2022-22721
CVE	CVE-2022-23943
XREF	IAVA:2022-A-0124-S

Plugin Information

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

Plugin Output

tcp/8585/www

```
URL              : http://10.0.2.8:8585/
Installed version : 2.2.21
Fixed version     : 2.4.53
```

193421 - Apache 2.4.x < 2.4.54 Authentication Bypass

Synopsis

The remote web server is affected by an authentication bypass vulnerability.

Description

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

- 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

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

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

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)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-31813
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
Fixed version     : 2.4.54
```

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.

- 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)

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

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.2

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P)

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-28614
CVE	CVE-2022-28615
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2022/06/08, Modified: 2024/04/18

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
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 Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.55 or later.

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)

CVSS v3.0 Temporal Score

7.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.5

CVSS v2.0 Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2006-20001
CVE	CVE-2022-36760
CVE	CVE-2022-37436
XREF	IAVA:2023-A-0047-S

Plugin Information

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

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
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 Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.56 or later.

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)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-25690
CVE	CVE-2023-27522
XREF	IAVA:2023-A-0124-S

Plugin Information

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

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
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 Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 or later.

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)

CVSS v3.0 Temporal Score

8.3 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

8.1

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-40438
XREF	IAVA:2021-A-0440-S
XREF	CISA-KNOWN-EXPLOITED:2021/12/15

Plugin Information

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

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
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 Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 or later.

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)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-34798
CVE	CVE-2021-39275
XREF	IAVA:2021-A-0440-S

Plugin Information

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

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
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.

See Also

https://archive.apache.org/dist/httpd/Announcement2.2.txt

Solution

Upgrade to a version of Apache HTTP Server that is currently supported.

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)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

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

Plugin Output

tcp/8585/www

```
URL                                  : http://10.0.2.8:8585/
Installed version                    : 2.2.21
Security End of Life                 : July 11, 2017
Time since Security End of Life (Est.) : >= 6 years
```

53514 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Synopsis

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

Description

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

See Also

https://www.nessus.org/u?361871b1

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

VPR Score

7.3

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

I

References

BID	47242
CVE	CVE-2011-0657
MSKB	2509553

XREF IAVA:2011-A-0039-S
XREF MSFT:MS11-030

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2011/04/21, Modified: 2023/10/17

Plugin Output

udp/5355/llmnr

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.

See Also

http://www.nessus.org/u?577af692

http://www.nessus.org/u?8e4e0b74

Solution

Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.

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)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.7

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

References

BID	108273

CVE	CVE-2019-0708
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CEA-ID:CEA-2020-0129
XREF	CEA-ID:CEA-2019-0326
XREF	CEA-ID:CEA-2019-0700

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2019/05/22, Modified: 2024/05/20

Plugin Output

tcp/3389/msrdp

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)

See Also

http://www.php.net/ChangeLog-5.php#5.3.15

Solution

Upgrade to PHP version 5.3.15 or later.

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	54612
BID	54638
CVE	CVE-2012-2688
CVE	CVE-2012-3365

Plugin Information

Published: 2012/07/20, Modified: 2024/05/28

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
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.

See Also

http://php.net/eol.php

https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported.

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)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2024/05/31

Plugin Output

tcp/8585/www

```
Source              : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version   : 5.3.10
```

```
    End of support date : 2014/08/14
    Announcement        : http://php.net/eol.php
    Supported versions  : 8.1.x / 8.2.x / 8.3.x
```

108797 - Unsupported Windows OS (remote)

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

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)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF	IAVA:0001-A-0501

Plugin Information

Published: 2018/04/03, Modified: 2023/07/27

Plugin Output

tcp/0

```
The following Windows version is installed and not supported:

Microsoft Windows Server 2008 R2 Standard Service Pack 1
```

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 Nessus has not tested for these flaws but has instead relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.23

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.23 or later.

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)

CVSS v3.0 Temporal Score

6.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.1 (CVSS2#E:U/RL:OF/RC:C)

References

BID	53046
BID	55131
CVE	CVE-2012-0883
CVE	CVE-2012-2687
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

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

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
```

```
    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 Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.zerodayinitiative.com/advisories/ZDI-14-236/

https://archive.apache.org/dist/httpd/CHANGES_2.2.29

http://httpd.apache.org/security/vulnerabilities_22.html

http://swende.se/blog/HTTPChunked.html

Solution

Upgrade to Apache version 2.2.29 or later.

Note that version 2.2.28 was never officially released.

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)

CVSS v3.0 Temporal Score

6.6 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	66550
BID	68678
BID	68742
BID	68745
CVE	CVE-2013-5704
CVE	CVE-2014-0118
CVE	CVE-2014-0226
CVE	CVE-2014-0231
XREF	EDB-ID:34133

Plugin Information

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

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
Fixed version     : 2.2.29
```

193422 - Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability

Synopsis

The remote web server is affected by a HTTP request smuggling vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by a http request smuggling vulnerability 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

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

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

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)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-26377
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
Fixed version     : 2.4.54
```

193423 - 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.

- 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

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

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

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)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-30522
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
Fixed version     : 2.4.54
```

193424 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)

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.

- 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)

- 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)

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

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

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)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-29404
CVE	CVE-2022-30556
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
Fixed version     : 2.4.54
```

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.

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

Solution

Upgrade to Apache version 2.4.58 or later.

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)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-43622
CVE	CVE-2023-45802
XREF	IAVA:2023-A-0572-S

Plugin Information

Published: 2023/10/19, Modified: 2024/04/29

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
Fixed version     : 2.4.58
```

193419 - Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)

Synopsis

The remote web server is affected by an out-of-bounds read vulnerability.

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.

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

Solution

Upgrade to Apache version 2.4.58 or later.

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)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-31122
XREF	IAVA:2023-A-0572-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/29

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
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 Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.59 or later.

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)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.0

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-38709
CVE	CVE-2024-24795
CVE	CVE-2024-27316
XREF	IAVA:2024-A-0202

Plugin Information

Published: 2024/04/04, Modified: 2024/06/07

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
Fixed version     : 2.4.59
```

58435 - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Synopsis

The remote Windows host could allow arbitrary code execution.

Description

An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.

See Also

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-020

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.

Risk Factor

High

VPR Score

9.6

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

BID	52353
BID	52354
CVE	CVE-2012-0002
CVE	CVE-2012-0152
MSKB	2621440
MSKB	2667402
XREF	EDB-ID:18606
XREF	MSFT:MS12-020
XREF	IAVA:2012-A-0039

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2012/03/22, Modified: 2024/05/20

Plugin Output

tcp/3389/msrdp

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

http://www.nessus.org/u?68fc8eff

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?065561d0

http://www.nessus.org/u?d9f569cf

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

http://www.nessus.org/u?b9d9ebf9

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions.

SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.7

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.1 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212

MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CISA-KNOWN-EXPLOITED:2022/08/10
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	CISA-KNOWN-EXPLOITED:2022/04/27
XREF	CISA-KNOWN-EXPLOITED:2022/06/14

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2017/03/20, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Sent:
00000054ff534d4225000000001803c800000000000000000000000000408244e0010000110000000
00ffffffff0000000000000000000000005400000054000200230000001100005c00500049005000
45005c0000000000

Received:
ff534d4225050200c09803c8000000000000000000000000000408244e00100001000000
```

10547 - Microsoft Windows LAN Manager SNMP LanMan Services Disclosure

Synopsis

The list of LanMan services running on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of LanMan services on the remote host by sending SNMP requests with the OID 1.3.6.1.4.1.77.1.2.3.1.1

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

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)

VPR Score

3.4

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

CVE	CVE-1999-0499

Plugin Information

Published: 2000/11/10, Modified: 2024/03/22

Plugin Output

udp/161/snmp

```
jmx
Power
Server
jenkins
```

```
IP Helper
DNS Client
wampapache
wampmysqld
DHCP Client
Workstation
SNMP Service
Plug and Play
Print Spooler
OpenSSH Server
Task Scheduler
Windows Update
Remote Registry
Windows Firewall
COM+ Event System
Windows Event Log
IPsec Policy Agent
Group Policy Client
Network Connections
RPC Endpoint Mapper
Software Protection
Network List Service
User Profile Service
Base Filtering Engine
Microsoft FTP Service
TCP/IP NetBIOS Helper
Cryptographic Services
Certificate Propagation
Remote Desktop Services
SPP Notification Service
Shell Hardware Detection
domain1 GlassFish Server
Diagnostic Policy Service
Security Accounts Manager
Network Location Awareness
Windows Font Cache Service
Remote Procedure Call (RPC)
DCOM Server Process Launcher
Remote Desktop Configuration
MEDC Server Component - Apache
Application Host Helper Service
Network Store Interface Service
Distributed Link Tracking Client
System Event Notification Service
World Wide Web Publishing Service
VirtualBox Guest Additions Service
Windows Management Instrumentation
Windows Process Activation Service
Distributed Transaction Coordinator
IKE and AuthIP IPsec Keying Modules
ManageEngine Desktop Central Server
Desktop Window Manager Session Manager
Windows Remote Management (WS-Management)
MEDC Server Component - Notification Server
Elasticsearch 1.1.1 (elasticsearch-service-x64)
Remote Desktop Services UserMode Port Redirector
```

59056 - PHP 5.3.x < 5.3.13 CGI Query String Code Execution

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.13 and, as such, is potentially affected by a remote code execution and information disclosure vulnerability.

The fix for CVE-2012-1823 does not completely correct the CGI query vulnerability. Disclosure of PHP source code and code execution via query parameters are still possible.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

https://bugs.php.net/bug.php?id=61910

http://www.php.net/archive/2012.php#id2012-05-08-1

http://www.php.net/ChangeLog-5.php#5.3.13

Solution

Upgrade to PHP version 5.3.13 or later. A 'mod_rewrite'
workaround is available as well.

Risk Factor

High

VPR Score

7.4

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	53388

CVE	CVE-2012-2311
CVE	CVE-2012-2335
CVE	CVE-2012-2336
XREF	CERT:520827

Exploitable With

Metasploit (true)

Plugin Information

Published: 2012/05/09, Modified: 2024/05/28

Plugin Output

tcp/8585/www

```
Version source     : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version  : 5.3.10
Fixed version      : 5.3.13
```

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)

See Also

http://www.nessus.org/u?ec6f812f

https://bugs.php.net/bug.php?id=61755

http://www.php.net/ChangeLog-5.php#5.3.14

http://www.nessus.org/u?99140286

http://www.nessus.org/u?a42ad63a

Solution

Upgrade to PHP version 5.3.14 or later.

Risk Factor

High

VPR Score

7.3

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	47545
BID	53729
BID	54777
BID	57462
CVE	CVE-2012-2143
CVE	CVE-2012-2386
CVE	CVE-2012-3450
CVE	CVE-2012-6113
XREF	EDB-ID:17201

Plugin Information

Published: 2012/06/15, Modified: 2024/05/31

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
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.

See Also

http://www.nessus.org/u?2dcf53bd

http://www.nessus.org/u?889595b1

http://www.php.net/ChangeLog-5.php#5.3.22

Solution

Upgrade to PHP version 5.3.22 or later.

Risk Factor

High

VPR Score

5.9

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	58224
BID	58766
CVE	CVE-2013-1635
CVE	CVE-2013-1643

Plugin Information

Published: 2013/03/04, Modified: 2024/05/28

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
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.

See Also

http://www.nessus.org/u?7c770707

http://www.php.net/ChangeLog-5.php#5.3.23

Solution

Upgrade to PHP version 5.3.23 or later.

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)

CVSS v3.0 Temporal Score

6.4 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	58224
BID	58766
BID	62373
CVE	CVE-2013-1635
CVE	CVE-2013-1643
CVE	CVE-2013-1824

Plugin Information

Published: 2013/05/24, Modified: 2024/05/28

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
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.

See Also

https://seclists.org/fulldisclosure/2013/Dec/96

https://bugzilla.redhat.com/show_bug.cgi?id=1036830

http://www.nessus.org/u?b6ec9ef9

http://www.php.net/ChangeLog-5.php#5.3.28

Solution

Upgrade to PHP version 5.3.28 or later.

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)

CVSS v3.0 Temporal Score

6.6 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	60843
BID	61776
BID	64225
CVE	CVE-2013-4073
CVE	CVE-2013-4248
CVE	CVE-2013-6420
XREF	EDB-ID:30395

Plugin Information

Published: 2013/12/14, Modified: 2024/05/31

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
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 Nessus 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.

See Also

http://php.net/archive/2014.php#id2014-08-14-1

http://www.php.net/ChangeLog-5.php#5.3.29

Solution

Upgrade to PHP version 5.3.29 or later.

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)

CVSS v3.0 Temporal Score

6.4 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	64018
BID	67759
BID	67765
BID	67837
BID	68007
BID	68120
BID	68237
BID	68238
BID	68239
BID	68241
BID	68243
BID	68423
BID	69271
BID	73385
CVE	CVE-2013-6712
CVE	CVE-2014-0207
CVE	CVE-2014-0237
CVE	CVE-2014-0238
CVE	CVE-2014-3478
CVE	CVE-2014-3479
CVE	CVE-2014-3480
CVE	CVE-2014-3487

CVE	CVE-2014-3515
CVE	CVE-2014-3981
CVE	CVE-2014-4049
CVE	CVE-2014-4721

Plugin Information

Published: 2014/08/20, Modified: 2024/05/31

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.29
```

58988 - PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.12 / 5.4.2, and as such is potentially affected by a remote code execution and information disclosure vulnerability.

An error in the file 'sapi/cgi/cgi_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

https://bugs.php.net/bug.php?id=61910

http://www.php.net/archive/2012.php#id2012-05-03-1

http://www.php.net/ChangeLog-5.php#5.3.12

http://www.php.net/ChangeLog-5.php#5.4.2

Solution

Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite'

workaround is available as well.

Risk Factor

High

VPR Score

9.2

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	53388
CVE	CVE-2012-1823
XREF	CERT:520827
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2012/05/04, Modified: 2024/05/31

Plugin Output

tcp/8585/www

```
Version source     : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version  : 5.3.10
Fixed version      : 5.3.12 / 5.4.2
```

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

See Also

https://www.php.net/ChangeLog-7.php#7.3.24

Solution

Upgrade to PHP version 7.3.24 or later.

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)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

STIG Severity

I

References

XREF	IAVA:2020-A-0510-S

Plugin Information

Published: 2020/11/06, Modified: 2024/06/04

Plugin Output

tcp/8585/www

```
  URL              : http://10.0.2.8:8585/ (5.3.10 under Server: Apache/2.2.21 (Win64) PHP/5.3.10
DAV/2, X-Powered-By: PHP/5.3.10)
  Installed version : 5.3.10
  Fixed version     : 7.3.24
```

41028 - SNMP Agent Default Community Name (public)

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

Risk Factor

High

VPR Score

5.2

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	2112
CVE	CVE-1999-0517

Plugin Information

Published: 2002/11/25, Modified: 2022/06/01

Plugin Output

udp/161/snmp

```
The remote SNMP server replies to the following default community
```

```
string :

public
```

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 Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

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)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.9

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
CVE	CVE-2005-4900
XREF	CERT:836068
XREF	CWE:310

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=metasploitable3-win2k8
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Feb 27 09:58:46 2024 GMT
Valid To            : Aug 28 09:58:46 2024 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQLBnqDDioto9I9KYf2ur/
rzANBgkqhkiG9w0BAQUFADAhMR8wHQYDVQQDExZtZXRhc3Bsb2l0YWJsZTMtd2luMms4MB4XDTI0MDIyNzA5NTg0NloXDTI0MDgyODA5NTg0NlowIT
Sml+2f609RoTGeIjqF3UrNSAVn3GJLmhAMybSWnJ3UEPjVhxqhXHx37WwB6EgqEuX0ift7JAQncSEDHwCf
+q0g52XEktoJNYpimbiAQCbXou2CTZQDmcAd+T80iJNoCfA71Mftom4L9Wdaa15f5peOmi+hDJFexfAHz34W2M/
IE3yommKbQW39PtdyeV
+3oG6KypJihACOM4PfMPIwq4APd98JdbNyDQMrBFTJB8i94wOoBlJx2Z6rYMzhnEGvcKI45X738jkCmQk5yGV2HI3T1ijUb0018nyb7f3L3YdntDZE
XAUqC46yvHyyKEbSTNYR+yMJZ/
rNDnUVsCAwEAAaMkMCIwEwYDVR0lBAwwCgYIKwYBBQUHAwEwCwYDVR0PBAQDAgQwMA0GCSqGSIb3DQEBBQUAA4IBAQAFD4s/
kXwGPwA4WKTbMcsaktP7LHwJ2I/
hCy4THgSDBNTb8EiahesFSU41YBhdGY1plSGArQIl3OdQLFksSplswWrVkr4099SqOO2MDup8U2odOKEQEIMl4X
+Aozt7Rc0N0nXQ2PPCNndKSHMsDFhwOPS53oMr2vTVvw18iOSX4TyXH5qocnUIfZsgxovVHzEyUnBNifL6K/9sg7x1adzMFF4ayX2SD7aXvapRTCvC
q76omo8FNoWzd8An8UqKH5GdUJfGlNxgYA2DojAFYi7nTlVUrvdmrXb7DVSGtZd5mafvulYrCJp4kE84CyQjead229GFNzSGn2+aB
-----END CERTIFICATE-----
```

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 Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

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)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.9

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
CVE	CVE-2005-4900
XREF	CERT:836068
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/8383/www

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

Subject             : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop Central/
E=support@desktopcentral.com
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Sep 08 12:24:44 2010 GMT
Valid To            : Sep 05 12:24:44 2020 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIID3TCCA0agAwIBAgIJAPWc73Hm23KlMA0GCSqGSIb3DQEBBQUAMIGmMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExEzARBgNVBAcTClBsZWFzYW
+WAUuldwD3YKmlgJIoyFB0SuCkOngoUmkVmsPS/
+LvKN09bPCa1BR0IXCKOSz2kOAayLsx0vMs2X9Jt74gk3WQIg59WYwtpKKried63w86mMWRayHe2uEGFArzNIKseZ0PpcNSqGPwgwKGTfrDuyCeFpD
+f8zyBAnYqkN5OrIXXY5S4Eu/HjCB2wYDVR0jBIHTMIHQgBT+f8zyBAnYqkN5OrIXXY5S4Eu/
HqGBrKSBqTCBpjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMRMwEQYDVQQHEwpQbGVhc2FudG9uMRkwFwYDVQQKExBab2hvIENvcnBvcmF0aW9uMR
MA0GCSqGSIb3DQEBBQUAA4GBAEXoUjGeAGFqUEmrwcwKyJ3um3Yw+ViJWnuCtsiSipqlcj1Ip+/
P5SN7RRR2MUUijiIZjnEguG7qr95qTuahPl8w+0nyfZVXm2yxkAwDSjuRP3pxAPUhkcXiA11jTnpeK3TCgX/Na
+eBNQCGT2LosP5A8aFT5yXOF7T/hxnZybr1
-----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. Nessus 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.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

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)

VPR Score

5.1

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-2016-2183

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}
```

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. Nessus 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.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

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)

VPR Score

5.1

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-2016-2183

Plugin Information

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

Plugin Output

tcp/8383/www

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    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}
```

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

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.22

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.22 or later.

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)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.6

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	49957
BID	50494
BID	50802
BID	51407
BID	51705
BID	51706
BID	56753
CVE	CVE-2011-3368
CVE	CVE-2011-3607
CVE	CVE-2011-4317
CVE	CVE-2012-0021
CVE	CVE-2012-0031
CVE	CVE-2012-0053
CVE	CVE-2012-4557

Plugin Information

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

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
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 Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.24

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.24 or later. Alternatively, ensure that the affected modules are not in use.

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)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.0

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	58165
CVE	CVE-2012-3499
CVE	CVE-2012-4558
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

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

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
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 Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.25

http://httpd.apache.org/security/vulnerabilities_22.html

http://www.nessus.org/u?f050c342

Solution

Upgrade to Apache version 2.2.25 or later. Alternatively, ensure that the affected modules are not in use.

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)

CVSS v3.0 Temporal Score

4.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.4

CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	59826
BID	61129
CVE	CVE-2013-1862
CVE	CVE-2013-1896

Plugin Information

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

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
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 Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.27

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.27 or later. Alternatively, ensure that the affected modules are not in use.

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)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	66303
CVE	CVE-2013-6438
CVE	CVE-2014-0098

Plugin Information

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

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Installed version : 2.2.21
Fixed version     : 2.2.27
```

193420 - Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)

Synopsis

The remote web server is affected by an out-of-bound read vulnerability

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by an out-of-bounds read vulnerability as referenced in the 2.4.54 advisory.

- 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

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

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

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)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-28330
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/8585/www

```
URL               : http://10.0.2.8:8585/
Installed version : 2.2.21
Fixed version     : 2.4.54
```

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

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)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
The following directories are browsable :

http://10.0.2.8:8585/uploads/
http://10.0.2.8:8585/uploads/1703xoR7.htm/
http://10.0.2.8:8585/uploads/1703xoR7.htm/9l0UyBC3.htm/
http://10.0.2.8:8585/uploads/1703xoR7.htm/9l0UyBC3.htm/RAoW4KDM.htm/
http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/
http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/
http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/V9D9Bwzx.htm/
http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/SFozlpWs.htm/
http://10.0.2.8:8585/uploads/1703xoR7.htm/QrcxOEde.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/
```

```
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/2WdwFypX.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/LCUVhZ7z.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/R2Mqyy6X.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/T9vq7fVh.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/xzrVs9l0.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/R2WdwFyp.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/RRnHOMMz.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/YDxVuZ14.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/dWikEPIR.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/lXGguc6o.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/vs60_iuJ.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/QE2A2sKS.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/gJJEBUus.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/ivCwebkg.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/pgRsHOfe.htm/
http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/pgRsH [...]
```

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.

See Also

http://www.nessus.org/u?e979b5cb

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

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)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.0

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	9506

BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

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

Plugin Output

tcp/8585/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.

Nessus sent the following TRACE request : \n\n------------------------------ snip
 ------------------------------\nTRACE /Nessus1637384240.html HTTP/1.1
Connection: Close
Host: 10.0.2.8
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: Thu, 27 Jun 2024 00:50:34 GMT
Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1637384240.html HTTP/1.1
Connection: Keep-Alive
Host: 10.0.2.8
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
```

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

http://www.nessus.org/u?52ade1e9

http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.0

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090
MSKB	3147461
MSKB	3147458
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information

Published: 2016/04/13, Modified: 2019/07/23

Plugin Output

tcp/49179/dce-rpc

10546 - Microsoft Windows LAN Manager SNMP LanMan Users Disclosure

Synopsis

The list of LanMan users of the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of LanMan users on the remote host by sending SNMP requests with the OID 1.3.6.1.4.1.77.1.2.25.1.1

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

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)

VPR Score

3.4

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-1999-0499

Plugin Information

Published: 2000/11/10, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
sshd
Guest
greedo
vagrant
```

```
han_solo
kylo_ren
boba_fett
chewbacca
ben_kenobi
jabba_hutt
artoo_detoo
c_three_pio
darth_vader
leia_organa
sshd_server
jarjar_binks
Administrator
luke_skywalker
anakin_skywalker
lando_calrissian
```

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.

See Also

http://www.nessus.org/u?60cbc5f0

http://www.nessus.org/u?8456482e

http://www.php.net/ChangeLog-5.php#5.3.26

Solution

Apply the vendor patch or upgrade to PHP version 5.3.26 or later.

Risk Factor

Medium

VPR Score

3.6

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	60411
BID	60731
CVE	CVE-2013-2110
CVE	CVE-2013-4635

Plugin Information

Published: 2013/06/07, Modified: 2024/05/31

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
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.

See Also

https://bugs.php.net/bug.php?id=64949

https://bugs.php.net/bug.php?id=65236

http://www.php.net/ChangeLog-5.php#5.3.27

Solution

Apply the vendor patch or upgrade to PHP version 5.3.27 or later.

Risk Factor

Medium

VPR Score

5.9

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	61128
CVE	CVE-2013-4113

Plugin Information

Published: 2013/07/12, Modified: 2024/05/31

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.27
```

58966 - PHP < 5.3.11 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 earlier than 5.3.11, and as such is potentially affected by multiple vulnerabilities :

- During the import of environment variables, temporary changes to the 'magic_quotes_gpc' directive are not handled properly. This can lower the difficulty for SQL injection attacks. (CVE-2012-0831)

- The '$_FILES' variable can be corrupted because the names of uploaded files are not properly validated. (CVE-2012-1172)

- The 'open_basedir' directive is not properly handled by the functions 'readline_write_history' and 'readline_read_history'.

- The 'header()' function does not detect multi-line headers with a CR. (Bug #60227 / CVE-2011-1398)

See Also

http://www.nessus.org/u?e81d4026

https://bugs.php.net/bug.php?id=61043

https://bugs.php.net/bug.php?id=54374

https://bugs.php.net/bug.php?id=60227

https://marc.info/?l=oss-security&m=134626481806571&w=2

http://www.php.net/archive/2012.php#id2012-04-26-1

http://www.php.net/ChangeLog-5.php#5.3.11

Solution

Upgrade to PHP version 5.3.11 or later.

Risk Factor

Medium

VPR Score

6.7

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	51954
BID	53403
BID	55297
CVE	CVE-2011-1398
CVE	CVE-2012-0831
CVE	CVE-2012-1172

Plugin Information

Published: 2012/05/02, Modified: 2024/05/28

Plugin Output

tcp/8585/www

```
Version source     : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version  : 5.3.10
Fixed version      : 5.3.11
```

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.

See Also

https://www.php.net/ChangeLog-7.php#7.3.28

Solution

Upgrade to PHP version 7.3.28 or later.

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)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2021/08/26, Modified: 2024/06/04

Plugin Output

tcp/8585/www

```
  URL               : http://10.0.2.8:8585/ (5.3.10 under Server: Apache/2.2.21 (Win64) PHP/5.3.10
DAV/2, X-Powered-By: PHP/5.3.10)
  Installed version : 5.3.10
  Fixed version     : 7.3.28
```

73289 - PHP PHP_RSHUTDOWN_FUNCTION Security Bypass

Synopsis

The remote web server uses a version of PHP that is potentially affected by a security bypass vulnerability.

Description

According to its banner, the version of PHP 5.x installed on the remote host is 5.x prior to 5.3.11 or 5.4.x prior to 5.4.1 and thus, is potentially affected by a security bypass vulnerability.

An error exists related to the function 'PHP_RSHUTDOWN_FUNCTION' in the libxml extension and the 'stream_close' method that could allow a remote attacker to bypass 'open_basedir' protections and obtain sensitive information.

Note that this plugin has not attempted to exploit this issue, but has instead relied only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?bcc428c2

https://bugs.php.net/bug.php?id=61367

Solution

Upgrade to PHP version 5.3.11 / 5.4.1 or later.

Risk Factor

Medium

VPR Score

3.4

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	65673
CVE	CVE-2012-1171

Plugin Information

Published: 2014/04/01, Modified: 2024/05/28

Plugin Output

tcp/8585/www

```
Version source    : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2, X-Powered-By: PHP/5.3.10
Installed version : 5.3.10
Fixed version     : 5.3.11 / 5.4.1
```

46803 - PHP expose_php Information Disclosure

Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.

Other such Easter eggs likely exist, but Nessus has not checked for them.

See Also

https://www.0php.com/php_easter_egg.php

https://seclists.org/webappsec/2004/q4/324

Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2010/06/03, Modified: 2022/04/11

Plugin Output

tcp/8585/www

```
Nessus was able to verify the issue using the following URL :

  http://10.0.2.8:8585/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

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.

See Also

http://www.nessus.org/u?8033da0d

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and

- On Microsoft Windows operating systems, select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

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)

VPR Score

2.5

CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	13818
CVE	CVE-2005-1794

Plugin Information

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

Plugin Output

tcp/3389/msrdp

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

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)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Synopsis

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

https://terrapin-attack.com/

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.1

CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:N/I:C/A:N)

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha1-etm@openssh.com
Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha1-etm@openssh.com
```

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 Nessus 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.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

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)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/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=metasploitable3-win2k8
|-Issuer  : CN=metasploitable3-win2k8
```

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 Nessus 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.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

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)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

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

Plugin Output

tcp/8383/www

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

|-Subject   : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop Central/
E=support@desktopcentral.com
|-Not After : Sep 05 12:24:44 2020 GMT

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 : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop Central/
E=support@desktopcentral.com
|-Issuer  : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop Central/
E=support@desktopcentral.com
```

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.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

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)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

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

Plugin Output

tcp/8383/www

```
The SSL certificate has already expired :

  Subject          : C=US, ST=CA, L=Pleasanton, O=Zoho Corporation, OU=ManageEngine, CN=Desktop
 Central, emailAddress=support@desktopcentral.com
  Issuer           : C=US, ST=CA, L=Pleasanton, O=Zoho Corporation, OU=ManageEngine, CN=Desktop
 Central, emailAddress=support@desktopcentral.com
  Not valid before : Sep  8 12:24:44 2010 GMT
  Not valid after  : Sep  5 12:24:44 2020 GMT
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

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)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/8383/www

```
The identities known by Nessus are :

  10.0.2.8
  metasploitable3-win2k8
  10.0.2.8

The Common Name in the certificate is :

  Desktop Central
```

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.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

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)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

4.4

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

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.

Solution

Purchase or generate a proper SSL certificate for this service.

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)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/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=metasploitable3-win2k8
```

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.

Solution

Purchase or generate a proper SSL certificate for this service.

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)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

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

Plugin Output

tcp/8383/www

```
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 : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop Central/
E=support@desktopcentral.com
```

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.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

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)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF CWE:327

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.
```

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.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

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)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/8383/www

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

157288 - TLS Version 1.1 Deprecated Protocol

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.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

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)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF	CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/8383/www

```
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.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)

http://www.nessus.org/u?e2628096

Solution

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

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)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2012/03/23, Modified: 2024/05/20

Plugin Output

tcp/3389/msrdp

```
Nessus 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.

Solution

Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2012/01/25, Modified: 2024/05/20

Plugin Output

tcp/3389/msrdp

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

2. Medium
```

57640 - Web Application Information Disclosure

Synopsis

The remote web application discloses path information.

Description

At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

Solution

Filter error messages containing path information.

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2012/01/25, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
The request GET /?phpinfo=1&lang=fr HTTP/1.1
Host: 10.0.2.8:8585
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*


produces the following path information :
<tr><td class="e">Compiler </td><td class="v">MSVC9 (Visual C++ 20 [...]
<tr><td class="e">Architecture </td><td class="v">x64 </td></tr>
[...] hared&quot; &quot;--with-oci8-11g=C:\php-sdk\php53dev\vc9\x64\deps\insta [...]
<tr><td class="e">Server API </td><td class="v">Apache 2.0 Handler [...]
<tr><td class="e">Virtual Directory Support </td><td class="v">ena [...]

The request GET /?phpinfo=1 HTTP/1.1
Host: 10.0.2.8:8585
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
```

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


produces the following path information :
<tr><td class="e">Compiler </td><td class="v">MSVC9 (Visual C++ 20 [...]
<tr><td class="e">Architecture </td><td class="v">x64 </td></tr>
[...] hared&quot; &quot;--with-oci8-11g=C:\php-sdk\php53dev\vc9\x64\deps\insta [...]
<tr><td class="e">Server API </td><td class="v">Apache 2.0 Handler [...]
<tr><td class="e">Virtual Directory Support </td><td class="v">ena [...]

The request GET /?lang=%00ydumnt&phpinfo=1 HTTP/1.1
Host: 10.0.2.8:8585
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*


produces the following path information :
<tr><td class="e">Compiler </td><td class="v">MSVC9 (Visual C++ 20 [...]
<tr><td class="e">Architecture </td><td class="v">x64 </td></tr>
[...] hared&quot; &quot;--with-oci8-1 [...]
```

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

https://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF	CWE:693

Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

tcp/8585/www

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://10.0.2.8:8585/wordpress/
```

90067 - WordPress User Enumeration

Synopsis

The remote web server contains a PHP application that is affected by an information disclosure vulnerability.

Description

The version of WordPress hosted on the remote web server is affected by a user enumeration vulnerability. An unauthenticated, remote attacker can exploit this to learn the names of valid WordPress users.

This information could be used to mount further attacks.

See Also

https://hackertarget.com/wordpress-user-enumeration/

Solution

n/a

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2016/03/21, Modified: 2024/06/05

Plugin Output

tcp/8585/www

```
Nessus was able to enumerate the following WordPress users from the WordPress install at
 'http://10.0.2.8:8585/wordpress' :
 admin
 vagrant
 user
 manager
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

4.2

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

Plugin Output

icmp/0

```
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in network format)
The difference between the local and remote clocks is -844 seconds.
```

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

https://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.9

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	74733

CVE	CVE-2015-4000
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/28, Modified: 2022/12/05

Plugin Output

tcp/8383/www

```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resourc [...]
```

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.

Solution

Change RDP encryption level to :

4. FIPS Compliant

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2008/02/11, Modified: 2024/05/20

Plugin Output

tcp/3389/msrdp

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

2. Medium (Client Compatible)
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus 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.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

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 :
  - metasploitable3-win2k8
```

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.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

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

Plugin Output

tcp/8585/www

```
URL        : http://10.0.2.8:8585/
Version    : 2.2.21
Source     : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
backported : 0
modules    : PHP/5.3.10 DAV/2
os         : Win64
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

42799 - Broken Web Servers

Synopsis

Tests on this web server have been disabled.

Description

The remote web server seems password protected or misconfigured. Further tests on it were disabled so that the whole scan is not slowed down.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/13, Modified: 2011/08/17

Plugin Output

tcp/8020/www

```
This web server was declared broken by :
 pytorch_torchserve_detect.nbin
for the following reason :
 The server answered with a 503 code (overloaded).
```

42799 - Broken Web Servers

Synopsis

Tests on this web server have been disabled.

Description

The remote web server seems password protected or misconfigured. Further tests on it were disabled so that the whole scan is not slowed down.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/13, Modified: 2011/08/17

Plugin Output

tcp/8383/www

```
This web server was declared broken by :
 pytorch_torchserve_detect.nbin
for the following reason :
 The server answered with a 503 code (overloaded).
```

47830 - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 's' parameter of the /wordpress/ CGI :

/wordpress/?s=%00ydumnt

-------- output --------
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width">
<title> ydumnt | Search Results  | Metasploit3</title>
<link rel="profile" href="http://gmpg.org/xfn/11">
<link rel="pingback" href="http://10.0.2.8:8585/wordpress/xmlrpc.php">
------------------------

+ The 'phpinfo' parameter of the / CGI :
```

```
/?phpinfo=%00ydumnt

-------- output --------
<tr><td class="e">SERVER_PROTOCOL </td><td class="v">HTTP/1.1 </td></tr>
<tr><td class="e">REQUEST_METHOD </td><td class="v">GET </td></tr>
<tr><td class="e">QUERY_STRING </td><td class="v">phpinfo=%00ydumnt </td
></tr>
<tr><td class="e">REQUEST_URI </td><td class="v">/?phpinfo=%00ydum [...]
<tr><td class="e">SCRIPT_NAME </td><td class="v">/index.php </td></tr>
------------------------

+ The 'lang' parameter of the / CGI :

/?lang=%00ydumnt&phpinfo=1

-------- output --------
<tr><td class="e">SERVER_PROTOCOL </td><td class="v">HTTP/1.1 </td></tr>
<tr><td class="e">REQUEST_METHOD </td><td class="v">GET </td></tr>
<tr><td class="e">QUERY_STRING </td><td class="v">lang=%00ydumnt&amp;php
info=1 </td></tr>
<tr><td class="e">REQUEST_URI </td><td class="v">/?lang=%00ydumnt& [...]
<tr><td class="e">SCRIPT_NAME </td><td class="v">/index.php </td></tr>
------------------------

+ The 'phpinfo' parameter of the / CGI :

/?lang=fr&phpinfo=%00ydumnt

-------- output --------
<tr><td class="e">SERVER_PROTOCOL </td><td class="v">HTTP/1.1 </td></tr>
<tr><td class="e">REQUEST_METHOD </td><td class="v">GET </td></tr>
<tr><td class="e">QUERY_STRING </td><td class="v">lang=fr&amp;phpinfo=%0
0ydumnt </td></tr>
<tr><td class="e">REQUEST_URI </td><td class="v">/?lang=fr&amp;php [...]
<tr><td class="e">SCRIPT_NAME </td><td class="v">/index.php </td></tr>
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to  [...]
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

Plugin Output

tcp/8585/www

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

XML injection                             : S=4          SP=4         AP=4         SC=2         AC=4

HTML injection                            : S=15         SP=15        AP=15        SC=5         AC=15

blind SQL injection                       : S=48         SP=48        AP=48        SC=24        AC=48

web code injection                        : S=4          SP=4         AP=4         SC=2         AC=4

cross-site scripting (comprehensive test): S=68          SP=68        AP=68        SC=34        AC=68

SQL injection                             : S=112        SP=112       AP=112       SC=56
 AC=112
unseen parameters                         : S=140        SP=140       AP=140       SC=70
 AC=140
SQL injection (2nd order)                 : S=4          SP=4         AP=4         SC=2         AC=4

directory traversal (extended test)       : S=204        SP=204       AP=204       SC=102
 AC=204
```

```
header injection                          : S=6          SP=6          AP=6          SC=2          AC=6
on site request forgery                   : S=3          SP=3          AP=3          SC=1          AC=3
local file inclusion                      : S=16         SP=16         AP=16         SC=8          AC=16
persistent XSS                            : S=16         SP=16         AP=16         SC=8          AC=16
SSI injection                             : S=12         SP=12         AP=12         SC=6          AC=12
HTTP response splitting                   : S=27         SP=27         AP=27         SC=9          AC=27
arbitrary command execution               : S=88         SP=88         AP=88         SC=44         AC=88
script injection                          : S=3          SP=3          AP=3          SC=1          AC=3
directory traversal (write access)     [...]
```

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 Nessus 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.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/06/24

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows_server_2008:r2:sp1 -> Microsoft Windows Server 2008

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.2.21 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:mysql:mysql -> MySQL MySQL
  cpe:/a:openbsd:openssh:7.1 -> OpenBSD OpenSSH
  cpe:/a:php:php:5.3.10 -> PHP PHP
  cpe:/a:wordpress:wordpress:4.6.1 -> WordPress
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/135/epmap

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0399C0

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0399C0

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
```

```
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-4b2c897c7f58258f3d

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc03B031

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc03B031

Object UUID : 14057355-446d-42d8-beb8-609e8faa114c
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-ba4f7b732bc549d91d

Object UUID : eb855cf7-af30-46cd-a3dd-522e0861184c
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-ba4f7b732bc549d91d

Object UUID : d2195d98-531f-4c66-983d [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/445/cifs

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\METASPLOITABLE3

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\METASPLOITABLE3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\METASPLOITABLE3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
```

```
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\METASPLOITABLE3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\METASPLOITABLE3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\METASPLOITABLE3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\METASPLOITABLE3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\METASPLOITABLE3

 [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49152/dce-rpc

```
The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 10.0.2.8
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49153/dce-rpc

```
The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 10.0.2.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 10.0.2.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 10.0.2.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
```

```
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 10.0.2.8
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49154/dce-rpc

```
The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.2.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.2.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.2.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
```

```
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.2.8

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.2.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 10.0.2.8
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49179/dce-rpc

```
The following DCERPC services are available on TCP port 49179 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49179
IP : 10.0.2.8
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49237/dce-rpc

```
The following DCERPC services are available on TCP port 49237 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49237
IP : 10.0.2.8
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49238/dce-rpc

```
The following DCERPC services are available on TCP port 49238 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49238
IP : 10.0.2.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
TCP Port : 49238
IP : 10.0.2.8
```

132634 - Deprecated SSLv2 Connection Attempts

Synopsis

Secure Connections, using a deprecated protocol were attempted as part of the scan

Description

This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities and most major ssl libraries such as openssl, nss, mbed and wolfssl do not provide this functionality in their latest versions. This protocol has been deprecated in Nessus 8.9 and later.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/01/06, Modified: 2020/01/06

Plugin Output

tcp/0

```
Nessus attempted the following SSLv2 connection(s) as part of this scan:

Plugin ID: 42476
Timestamp: 2024-06-27 00:47:32
Port: 22
```

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).

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

08:00:27:41:0F:1C : PCS Systemtechnik GmbH
08:00:27:12:95:5B : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:41:0F:1C
  - DA:D6:20:52:41:53
  - 08:00:27:12:95:5B
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

tcp/8585/www

```
24 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://10.0.2.8:8585/wordpress/         - /wordpress/
http://10.0.2.8:8585/wordpress/index.php/2016/09/ - /wordpress/
http://10.0.2.8:8585/wordpress/index.php/2016/09/26/hello-world/ - /wordpress/
http://10.0.2.8:8585/wordpress/index.php/2016/09/26/hello-world/#respond - /wordpress/
http://10.0.2.8:8585/wordpress/index.php/author/admin/ - /wordpress/
http://10.0.2.8:8585/wordpress/index.php/category/uncategorized/ - /wordpress/
http://10.0.2.8:8585/wordpress/index.php/comments/feed/ - /wordpress/
http://10.0.2.8:8585/wordpress/index.php/feed/ - /wordpress/
http://10.0.2.8:8585/wordpress/index.php/king-of-hearts/ - /wordpress/
http://10.0.2.8:8585/wordpress/wp-content/themes/twentyfourteen/genericons/genericons.css?ver=3.0.3
 - /wordpress/
http://10.0.2.8:8585/wordpress/wp-content/themes/twentyfourteen/style.css?ver=4.6.1 - /wordpress/
http://10.0.2.8:8585/wordpress/wp-includes/wlwmanifest.xml - /wordpress/
http://10.0.2.8:8585/wordpress/wp-json/ - /wordpress/
http://10.0.2.8:8585/wordpress/wp-login.php - /wordpress/
http://10.0.2.8:8585/wordpress/xmlrpc.php - /wordpress/
http://10.0.2.8:8585/wordpress/xmlrpc.php?rsd - /wordpress/
http://fonts.googleapis.com             - /wordpress/
http://gmpg.org/xfn/11                  - /wordpress/
http://s.w.org                          - /wordpress/
http://www.alterway.fr                  - /
http://www.wampserver.com               - /
http://www.wampserver.com/en/donations.php - /
https://fonts.googleapis.com/css?family=Lato%3A300%2C400%2C700%2C900%2C300italic%2C400italic
%2C700italic&subset=latin%2Clatin-ext - /wordpress/
https://wordpress.org/                  - /wordpress/
```

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.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8585/www

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

  - HTTP methods COPY DELETE GET HEAD LOCK MOVE OPTIONS POST PROPFIND
    PROPPATCH TRACE UNLOCK are allowed on :

    /uploads
    /uploads/1703xoR7.htm
    /uploads/1703xoR7.htm/9l0UyBC3.htm
    /uploads/1703xoR7.htm/9l0UyBC3.htm/RAoW4KDM.htm
    /uploads/1703xoR7.htm/KHtOAs4H.htm
    /uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm
    /uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/V9D9Bwzx.htm
    /uploads/1703xoR7.htm/KHtOAs4H.htm/SFozlpWs.htm
    /uploads/1703xoR7.htm/QrcxOEde.htm
    /uploads/1IXeyCeN.htm
    /uploads/1IXeyCeN.htm/4tWwXWQ0.htm
    /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm
    /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/2WdwFypX.htm
    /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/LCUVhZ7z.htm


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /cgi-bin

  - HTTP methods COPY DELETE GET HEAD MKCOL MKWORKSPACE MOVE NOTIFY
    OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /uploads
    /uploads/1703xoR7.htm
    /uploads/1703xoR7.htm/9l0UyBC3.htm
    /uploads/1703xoR7.htm/9l0UyBC3.htm/RAoW4KDM.htm
    /uploads/1703xoR7.htm/KHtOAs4H.htm
    /uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm
    /uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/V9D9Bwzx.htm
    /uploads/1703xoR7.htm/KHtOAs4H.htm/SFozlpWs.htm
    /uploads/1703xoR7.htm/QrcxOEde.htm
    /uploads/1IXeyCeN.htm
    /uploads/1IXeyCeN.htm/4tWwXWQ0.htm
    /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm
    /uploads/1IXeyCeN.ht [...]
```

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.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/8585/www

```
The remote web server type is :

Apache/2.2.21 (Win64) PHP/5.3.10 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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8585/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: Thu, 27 Jun 2024 00:51:55 GMT
  Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
  X-Powered-By: PHP/5.3.10
  Content-Length: 4462
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html lang="en" xml:lang="en">
<head>
<title>WAMPSERVER Homepage</title>
<meta http-equiv="Content-Type" content="txt/html; charset=utf-8" />
```

```
<style type="text/css">
* {
margin: 0;
padding: 0;
}
html {
background: #ddd;
}
body {
margin: 1em 10%;
padding: 1em 3em;
font: 80%/1.4 tahoma, arial, helvetica, lucida sans, sans-serif;
border: 1px solid #999;
background: #eee;
position: relative;
}
#head {
margin-bottom: 1.8em;
margin-top: 1.8em;
padding-bottom: 0em;
border-bottom: 1px solid #999;
letter-spacing: -500em;
text-indent: -500em;
height: 125px;
background: url(index.php?img=gifLogo) 0 0 no-repeat;
}
.utility {
position: absolute;
right: 4em;
top: 145px;
font-size: 0.85em;
}
.utility li {
display: inline;
}
h2 {
margin: 0.8em 0 0 0;
}
ul {
list-style: none;
margin: 0;
padding: 0;
}
#head ul li, dl ul li, #foot li {
list-style: none;
display: inline;
margin: 0;
padding: 0 0.2em;
}
ul.vhosts, ul.aliases, ul.projects, ul.tools {
list-style: none;
line-height: 24px;
}
ul.vhosts a, ul.aliases a, ul.projects a, ul.tools a {
padding-left: 22px;
background: url(index.php?img=pngFolder) 0 100% no-repeat;
}
ul.tools a {
background: url(index.php?img=pngWrench) 0 100% no-repeat;
}
ul.aliases a {
background: url(index.php?img=pngFolderGo) 0 100% no-repeat;
}
ul.vhosts a {
background: url(index.php?img=pngFolderGo) 0 100% no-repeat;
}
dl {
m [...]
```

14788 - IP Protocols Scan

Synopsis

This plugin detects the protocols understood by the remote IP stack.

Description

This plugin detects the protocols understood by the remote IP stack.

See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
4IP
6TCP
17UDP
41IPv6
50ESP
51AH
```

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

http://www.nessus.org/u?51eae65d

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2011/04/21, Modified: 2023/10/17

Plugin Output

udp/5355/llmnr

```
According to LLMNR, the name of the remote host is 'metasploitable3-win2k8'.
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows Server 2008 R2 Standard 7601 Service Pack 1
The remote native LAN manager is : Windows Server 2008 R2 Standard 6.1
The remote SMB Domain Name is : METASPLOITABLE3
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0506

Plugin Information

Published: 2007/10/04, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
Could not connect to the registry because:
Could not connect to \winreg
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

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

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

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

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7

The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://10.0.2.8:8585/
  - http://10.0.2.8:8585/index.php
  - http://10.0.2.8:8585/uploads/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/9l0UyBC3.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/9l0UyBC3.htm/RAoW4KDM.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/V9D9Bwzx.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/SFozlpWs.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/QrcxOEde.htm/
```

```
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/2WdwFypX.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/LCUVhZ7z.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/R2Mqyy6X.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/T9vq7fVh.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/xzrVs9l0.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/R2WdwFyp.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/RRnHOMMz.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/YDxVuZ14.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/dWikEPIR.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/lXGguc6o.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/vs60_iuJ.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/QE2A2sKS.htm/
- http://10.0.2.8:8585/upload [...]
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

https://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/8585/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://10.0.2.8:8585/
  - http://10.0.2.8:8585/index.php
  - http://10.0.2.8:8585/uploads/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/9l0UyBC3.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/9l0UyBC3.htm/RAoW4KDM.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/V9D9Bwzx.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/SFozlpWs.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/QrcxOEde.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/2WdwFypX.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/LCUVhZ7z.htm/
```

```
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/R2Mqyy6X.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/T9vq7fVh.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/xzrVs9l0.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/R2WdwFyp.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/RRnHOMMz.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/YDxVuZ14.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/dWikEPIR.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/lXGguc6o.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/vs60_iuJ.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/QE2A2sKS.htm/
- http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0. [...]
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/0

```
Nessus SNMP scanner was able to retrieve the open port list
with the community name: p*****
It found 15 open TCP ports and 9 open UDP ports.
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/135/epmap

```
Port 135/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/137/netbios-ns

```
Port 137/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/138

```
Port 138/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
Port 161/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/500

```
Port 500/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/3306/mysql

```
Port 3306/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/3389/msrdp

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

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/4500

```
Port 4500/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/5353

```
Port 5353/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/5355/llmnr

```
Port 5355/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/8020/www

```
Port 8020/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/8027

```
Port 8027/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/8383/www

```
Port 8383/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/8585/www

```
Port 8585/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/33848

```
Port 33848/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49152/dce-rpc

```
Port 49152/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49153/dce-rpc

```
Port 49153/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49154/dce-rpc

```
Port 49154/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49179/dce-rpc

```
Port 49179/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49237/dce-rpc

```
Port 49237/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49238/dce-rpc

```
Port 49238/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/54328

```
Port 54328/udp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/06/04

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.7.4
Nessus build : 20055
Plugin feed version : 202406261738
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : Reto_4_exex__Spring_4_CN
```

```
Scan policy used : Basic Network Scan
Scanner IP : 10.0.2.15
Port scanner(s) : snmp_scanner
Port range : 1-65535
Ping RTT : 152.085 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 2
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 : enabled
Web application tests : enabled
Web app tests -  Test mode : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/6/27 2:45 CEST
Scan duration : 1890 sec
Scan for malware : no
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

References

XREF IAVB:0001-B-0505

Plugin Information

Published: 2007/03/12, Modified: 2020/09/22

Plugin Output

tcp/0

```
It was not possible to connect to '\\METASPLOITABLE3\ADMIN$' with the supplied credentials.
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2024/06/19

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2008 R2 Standard Service Pack 1
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SSH:!:SSH-2.0-OpenSSH_7.1
SNMP:Hardware: Intel64 Family 6 Model 165 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version
 6.1 (Build 7601 Multiprocessor Free)
RDP:000000000f0000001000010008000100090000000100100010 0010
ICMP:!:::0:1:0:128:1:128:1:0:::0::1:>64:128:0:1:1:2:1:1:1:1:1:128:8192:MNWST:8:1:1
HTTP:!:Server: Apache

SinFP:!:
   P1:B11113:F0x12:W8192:O0204ffff:M1460:
   P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190804_7_p=49152
SSLcert:!:i/CN:Desktop Centrali/O:Zoho Corporationi/OU:ManageEngines/CN:Desktop Centrals/O:Zoho
 Corporations/OU:ManageEngine
701e2e6df8854c4f0b298dff03a2c6f0bac7d315
i/CN:metasploitable3-win2k8s/CN:metasploitable3-win2k8
8c4a607ee2eb6688536e1479ad13a9c9ae7c0c1b
```

```
The remote host is running Microsoft Windows Server 2008 R2 Standard Service Pack 1
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SMB service.
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2024/06/26

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 7.1
Banner  : SSH-2.0-OpenSSH_7.1
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/8383/www

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2024/05/31

Plugin Output

tcp/8585/www

```
Nessus was able to identify the following PHP version information :

  Version : 5.3.10
  Source  : Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
  Source  : X-Powered-By: PHP/5.3.10
```

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.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/06/11

Plugin Output

tcp/0

```
. You need to take the following 4 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 the following 51 different vulnerabilities :
CVE-2024-27316, CVE-2024-24795, CVE-2023-45802, CVE-2023-43622, CVE-2023-38709
CVE-2023-31122, CVE-2023-27522, CVE-2023-25690, CVE-2022-37436, CVE-2022-36760
CVE-2022-31813, CVE-2022-30556, CVE-2022-30522, CVE-2022-29404, CVE-2022-28615
CVE-2022-28614, CVE-2022-28330, CVE-2022-26377, CVE-2022-23943, CVE-2022-22721
CVE-2022-22720, CVE-2022-22719, CVE-2021-40438, CVE-2021-39275, CVE-2021-34798
CVE-2017-9788, CVE-2017-7679, CVE-2017-7668, CVE-2017-7659, CVE-2017-3169
CVE-2017-3167, CVE-2014-0231, CVE-2014-0226, CVE-2014-0118, CVE-2014-0098
CVE-2013-6438, CVE-2013-5704, CVE-2013-1896, CVE-2013-1862, CVE-2012-4558
CVE-2012-4557, CVE-2012-3499, CVE-2012-2687, CVE-2012-0883, CVE-2012-0053
CVE-2012-0031, CVE-2012-0021, CVE-2011-4317, CVE-2011-3607, CVE-2011-3368
CVE-2006-20001


[ 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.
```

```
+ Impact : Taking this action will resolve the following 2 different vulnerabilities :
CVE-2012-0152, CVE-2012-0002


[ 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 the following 35 different vulnerabilities :
CVE-2014-4721, CVE-2014-4049, CVE-2014-3981, CVE-2014-3515, CVE-2014-3487
CVE-2014-3480, CVE-2014-3479, CVE-2014-3478, CVE-2014-0238, CVE-2014-0237
CVE-2014-0207, CVE-2013-6712, CVE-2013-6420, CVE-2013-4635, CVE-2013-4248
CVE-2013-4113, CVE-2013-4073, CVE-2013-2110, CVE-2013-1824, CVE-2013-1643
CVE-2013-1635, CVE-2012-6113, CVE-2012-3450, CVE-2012-3365, CVE-2012-2688
CVE-2012-2386, CVE-2012-2336, CVE-2012-2335, CVE-2012-2311, CVE-2012-2143
CVE-2012-1823, CVE-2012-1172, CVE-2012-1171, CVE-2012 [...]
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/22, Modified: 2024/05/20

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.

Solution

Disable the service if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

35296 - SNMP Protocol Version Detection

Synopsis

This plugin reports the protocol version negotiated with the remote SNMP agent.

Description

By sending an SNMP 'get-next-request', it is possible to determine the protocol version of the remote SNMP agent.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2019/11/22

Plugin Output

udp/161/snmp

```
Nessus has negotiated SNMP communications at SNMPv2c.
```

19763 - SNMP Query Installed Software Disclosure

Synopsis

The list of software installed on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of installed software on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.25.6.3.1.2

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2005/09/20, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
7-Zip 22.01 (x64)
OpenSSH for Windows 7.1p1-1 (remove only)
Oracle VM VirtualBox Guest Additions 7.0.14
Microsoft .NET Framework 4.5.2
Java 8 Update 251 (64-bit)
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161
Java SE Development Kit 8 Update 211 (64-bit)
Microsoft .NET Framework 4.5.2
```

34022 - SNMP Query Routing Information Disclosure

Synopsis

The list of IP routes on the remote host can be obtained via SNMP.

Description

It is possible to obtain the routing information on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.4.21

An attacker may use this information to gain more knowledge about the network topology.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2008/08/21, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
10.0.2.0/255.255.255.0
10.0.2.8/255.255.255.255
10.0.2.255/255.255.255.255
127.0.0.0/255.0.0.0
127.0.0.1/255.255.255.255
127.255.255.255/255.255.255.255
224.0.0.0/240.0.0.0
255.255.255.255/255.255.255.255
```

10550 - SNMP Query Running Process List Disclosure

Synopsis

The list of processes running on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of running processes on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.25.4.2.1.2

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2000/11/13, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
  PID   CPU   MEM COMMAND           ARGS
    1 13359    24 System Idle Process
    4    41   100 System
  132     2 29076 svchost.exe
  252     0   476 smss.exe
  340     1  1192 csrss.exe       ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On
SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User
  392     0  1084 wininit.exe
  404     0  1116 csrss.exe       ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On
SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User
  448     0   148 winlogon.exe
  484     2 12300 explorer.exe
  492     0  3616 services.exe
  508     2  6276 lsass.exe
  516     0  3040 lsm.exe
  612     0  2868 svchost.exe
  628     0  3188 svchost.exe
  672     0  2172 VBoxService.exe
  740     0  3124 svchost.exe
  828     0  6368 svchost.exe
  888     0  9580 svchost.exe
  932     0  4284 svchost.exe
  988     0  1892 svchost.exe
 1120     0  1796 spoolsv.exe
 1148     0   904 svchost.exe
 1180     0  2164 wrapper.exe
```

```
  1204     0  2376 DesktopCentral.exe
  1260     0   128 cmd.exe           /c "C:\Program Files\jmx\start_jmx.bat"
  1348     0   252 conhost.exe
  1364     0  1504 domain1Service.exe
  1416    31 255068 elasticsearch-service-x64.exe  //RS//elasticsearch-service-x64
  1424     0   272 conhost.exe
  1428     1  4452 java.exe          -Dcom.sun.management.jmxremote -
Dcom.sun.management.jmxremote.port=1617 -Dcom.sun.management.jmxremote.authenticate=false -Dco
  1456     0  1084 svchost.exe
  1480     2 16332 jenkins.exe
  1532     0   872 cmd.exe         /c ""C:/glassfish/glassfish4/glassfish/lib/nadmin.bat"  start-
domain --watchdog --domaindir C:\\glassfish\\glassfish4\\glassfish
  1540     0   244 conhost.exe
  1584     1  1240 java.exe         -jar "C:\glassfish\glassfish4\glassfish\lib\..\modules\admin-
cli.jar" start-domain --watchdog --domaindir C:\\glassfish\\glassf
  1608     0   272 conhost.exe
  1692    [...]
```

10800 - SNMP Query System Information Disclosure

Synopsis

The System Information of the remote host can be obtained via SNMP.

Description

It is possible to obtain the system information about the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.1.1.

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2001/11/06, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
System information :
 sysDescr     : Hardware: Intel64 Family 6 Model 165 Stepping 2 AT/AT COMPATIBLE - Software: Windows
 Version 6.1 (Build 7601 Multiprocessor Free)
 sysObjectID  : 1.3.6.1.4.1.311.1.1.3.1.2
 sysUptime    : 0d 0h 25m 31s
 sysContact   :
 sysName      : metasploitable3-win2k8
 sysLocation  :
 sysServices  : 76
```

10551 - SNMP Request Network Interfaces Enumeration

Synopsis

The list of network interfaces cards of the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of the network interfaces installed on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.2.1.0

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2000/11/13, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
Interface 1 information :
ifIndex       : 1
ifDescr       : Software Loopback Interface 1
```

185519 - SNMP Server Detection

Synopsis

An SNMP server is listening on the remote host.

Description

The remote service is an SNMP agent which provides management data about the device.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2023/11/14, Modified: 2023/11/14

Plugin Output

udp/161/snmp

```
Nessus detected the following SNMP versions:
  - SNMPv1 (public community)
  - SNMPv1 (configured community)
  - SNMPv2c (public community)
  - SNMPv2c (configured community)
```

40448 - SNMP Supported Protocols Detection

Synopsis

This plugin reports all the protocol versions successfully negotiated with the remote SNMP agent.

Description

Extend the SNMP settings data already gathered by testing for\ SNMP versions other than the highest negotiated.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/31, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
This host supports SNMP version SNMPv1.
This host supports SNMP version SNMPv2c.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp521
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
```

```
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.1
SSH supported authentication : publickey,password,keyboard-interactive
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

```
This port supports TLSv1.0.
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8383/www

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

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/8383/www

```
The host name known by Nessus is :

  metasploitable3

The Common Name in the certificate is :

  desktop central
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: metasploitable3-win2k8

Issuer Name:

Common Name: metasploitable3-win2k8

Serial Number: 2C 19 EA 0C 38 A8 B6 8F 48 F4 A6 1F DA EA FF AF

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 27 09:58:46 2024 GMT
Not Valid After: Aug 28 09:58:46 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 DF D2 9A 5F B6 7F AD 3D 46 84 C6 78 88 EA 17 75 2B 35 20
            15 9F 71 89 2E 68 40 33 26 D2 5A 72 77 50 43 E3 56 1C 6A 85
            71 F1 DF B5 B0 07 A1 20 A8 4B 97 D2 27 ED EC 90 10 9D C4 84
            0C 7C 02 7F EA B4 83 9D 97 12 4B 68 24 D6 29 8A 66 E2 01 00
            9B 5E 8B B6 09 36 50 0E 67 00 77 E4 FC D2 22 4D A0 27 C0 EF
            53 1F B6 89 B8 2F D5 9D 69 AD 79 7F 9A 5E 3A 68 BE 84 32 45
            7B 17 C0 1F 3D F8 5B 63 3F 20 4D F2 A2 69 8A 6D 05 B7 F4 FB
            5D C9 E5 7E DE 81 BA 2B 2A 49 8A 10 02 38 CE 0F 7C C3 C8 C2
            AE 00 3D DF 7C 25 D6 CD C8 34 0C AC 11 53 24 1F 22 F7 8C 0E
            A0 19 49 C7 66 7A AD 83 33 86 71 06 BD C2 88 E3 95 FB DF C8
            E4 0A 64 24 E7 21 95 D8 72 37 4F 58 A3 51 BD 34 D7 C9 F2 6F
```

```
             B7 F7 2F 76 1D 9E D0 D9 13 41 67 5B F5 C0 52 A0 B8 EB 2B C7
             CB 22 84 6D 24 CD 61 1F B2 30 96 7F AC D0 E7 51 5B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 05 0F 8B 3F 91 7C 06 3F 00 38 58 A4 DB 31 CB 1A 92 D3 FB
           2C 7C 09 D8 8F E1 0B 2E 13 1E 04 83 04 D4 DB F0 48 9A 85 EB
           05 49 4E 35 60 18 5D 19 8D 69 95 21 80 AD 02 25 DC E7 50 2C
           59 2C 4A 99 6C C1 6A D5 92 BE 34 F7 D4 AA 38 ED 8C 0E EA 7C
           53 6A 1D 38 A1 10 10 83 25 E1 7F 80 A3 3B 7B 45 CD 0D D2 75
           D0 D8 F3 C2 36 77 4A 48 73 2C 0C 58 70 38 F4 B9 DE 83 2B DA
           F4 D5 BF 0D 7C 88 E4 97 E1 3C 97 1F 9A A8 72 75 08 7D 9B 20
           C6 8B D5 1F 31 32 52 70 4D 89 F2 FA 2B FF 6C 83 BC 75 69 DC
           CC 14 5E 1A C9 7D 92 0F B6 97 BD AA 51 4C 2B C2 94 20 FD 48
           1F EA  [...]
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8383/www

```
Subject Name:

Country: US
State/Province: CA
Locality: Pleasanton
Organization: Zoho Corporation
Organization Unit: ManageEngine
Common Name: Desktop Central
Email Address: support@desktopcentral.com

Issuer Name:

Country: US
State/Province: CA
Locality: Pleasanton
Organization: Zoho Corporation
Organization Unit: ManageEngine
Common Name: Desktop Central
Email Address: support@desktopcentral.com

Serial Number: 00 F5 9C EF 71 E6 DB 72 A5

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Sep 08 12:24:44 2010 GMT
Not Valid After: Sep 05 12:24:44 2020 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 F9 60 14 BA 57 70 0F 76 0A 9A 58 09 22 8C 85 07 44 AE 0A
            43 A7 82 85 26 91 59 AC 3D 2F FE 2E F2 8D D3 D6 CF 09 AD 41
            47 42 17 08 A3 92 CF 69 0E 01 AC 8B B3 1D 2F 32 CD 97 F4 9B
            7B E2 09 37 59 02 20 E7 D5 98 C2 DA 4A 2A B8 9E 77 AD F0 F3
            A9 8C 59 16 B2 1D ED AE 10 61 40 AF 33 48 2A C7 99 D0 FA 5C
            35 2A 86 3F 08 30 28 64 DF AC 3B B2 09 E1 69 0C 83 95 DB 81
            35 A5 48 B0 5E 06 0D 20 33
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 45 E8 52 31 9E 00 61 6A 50 49 AB C1 CC 0A C8 9D EE 9B 76
           30 F9 58 89 5A 7B 82 B6 C8 92 8A 9A A5 72 3D 48 A7 EF CF E5
           23 7B 45 14 76 31 45 22 8E 22 19 8E 71 20 B8 6E EA AF DE 6A
           4E E6 A1 3E 5F 30 FB 49 F2 7D 95 57 9B 6C B1 90 0C 03 4A 3B
           91 3F 7A 71 00 F5 21 91 C5 E2 03 5D 63 4E 7A 5E 2B 74 C2 81
           7F CD 6B E7 81 35 00 86 4F 62 E8 B0 FE 40 F1 A1 53 E7 25 CE
           17 B4 FF 87 19 D9 C9 BA F5

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: FE 7F CC F2 04 09 D8 AA 43 79 3A B2 17 5D 8E 52 E0 4B BF 1E


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: FE 7F CC F2 04 09 D8 AA 43 79 3A B2 17 5D 8E 52 E0 4B BF 1E
Country: US
State/Province: CA
Locality: Pleasanton
Organization: Zoho Corporation
Organizatio [...]
```

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.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

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

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.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8383/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
    ----------------------        ----------        ---           ----     ----------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          RSA      3DES-CBC(168)
 SHA1
    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-SHA            0x00, 0x33      DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39      DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45      DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88      DH            RSA      Camellia-CBC(256)
SHA1
   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
   CAMELLIA128-SHA               0x00, 0x41      RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84      RSA           RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67      DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x [...]
```

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.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

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 : 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.
```

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.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8383/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
    ----------------------        ----------        ---           ----     ---------------------   ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          RSA      3DES-CBC(168)
 SHA1
    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
```

```
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH           RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH           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
   DHE-RSA-AES128-SHA            0x00, 0x33       DH             RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH             RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH             RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH             RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH           RSA    [...]
```

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.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

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
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
 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}
```

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.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8383/www

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

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

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          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
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH         RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH         RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA            0x00, 0x33       DH           RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH           RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH           RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH           RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH         RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH         RSA      AES-CBC(256)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH           RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH           RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA25 [...]
```

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.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/8383/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop
 Central/E=support@desktopcentral.com
|-Issuer              : C=US/ST=CA/L=Pleasanton/O=Zoho Corporation/OU=ManageEngine/CN=Desktop
 Central/E=support@desktopcentral.com
|-Valid From          : Sep 08 12:24:44 2010 GMT
|-Valid To            : Sep 05 12:24:44 2020 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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

```
This port supports resuming 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.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

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
    ----------------------        ----------        ---           ----     ---------------------   ---
    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}
```

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.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8383/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
    ----------------------        ----------        ---           ----     --------------------    ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          RSA      3DES-CBC(168)
SHA1
    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
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45        DH            RSA      Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88        DH            RSA      Camellia-CBC(256)
SHA1
    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)
[...]
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus 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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus 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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3306/mysql

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus 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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8020/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus 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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8383/www

```
A TLSv1 server answered on this port.
```

tcp/8383/www

```
A web server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus 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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8585/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.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

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.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/8383/www

```
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.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8383/www

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

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

Plugin Output

tcp/0

```
SMB was detected on port 445 but no credentials were provided.
SMB local checks were not enabled.
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: metasploitable3-win2k8

Issuer Name:

Common Name: metasploitable3-win2k8

Serial Number: 2C 19 EA 0C 38 A8 B6 8F 48 F4 A6 1F DA EA FF AF

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 27 09:58:46 2024 GMT
Not Valid After: Aug 28 09:58:46 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 DF D2 9A 5F B6 7F AD 3D 46 84 C6 78 88 EA 17 75 2B 35 20
            15 9F 71 89 2E 68 40 33 26 D2 5A 72 77 50 43 E3 56 1C 6A 85
            71 F1 DF B5 B0 07 A1 20 A8 4B 97 D2 27 ED EC 90 10 9D C4 84
            0C 7C 02 7F EA B4 83 9D 97 12 4B 68 24 D6 29 8A 66 E2 01 00
            9B 5E 8B B6 09 36 50 0E 67 00 77 E4 FC D2 22 4D A0 27 C0 EF
            53 1F B6 89 B8 2F D5 9D 69 AD 79 7F 9A 5E 3A 68 BE 84 32 45
            7B 17 C0 1F 3D F8 5B 63 3F 20 4D F2 A2 69 8A 6D 05 B7 F4 FB
            5D C9 E5 7E DE 81 BA 2B 2A 49 8A 10 02 38 CE 0F 7C C3 C8 C2
            AE 00 3D DF 7C 25 D6 CD C8 34 0C AC 11 53 24 1F 22 F7 8C 0E
            A0 19 49 C7 66 7A AD 83 33 86 71 06 BD C2 88 E3 95 FB DF C8
            E4 0A 64 24 E7 21 95 D8 72 37 4F 58 A3 51 BD 34 D7 C9 F2 6F
```

```
            B7 F7 2F 76 1D 9E D0 D9 13 41 67 5B F5 C0 52 A0 B8 EB 2B C7
            CB 22 84 6D 24 CD 61 1F B2 30 96 7F AC D0 E7 51 5B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 05 0F 8B 3F 91 7C 06 3F 00 38 58 A4 DB 31 CB 1A 92 D3 FB
           2C 7C 09 D8 8F E1 0B 2E 13 1E 04 83 04 D4 DB F0 48 9A 85 EB
           05 49 4E 35 60 18 5D 19 8D 69 95 21 80 AD 02 25 DC E7 50 2C
           59 2C 4A 99 6C C1 6A D5 92 BE 34 F7 D4 AA 38 ED 8C 0E EA 7C
           53 6A 1D 38 A1 10 10 83 25 E1 7F 80 A3 3B 7B 45 CD 0D D2 75
           D0 D8 F3 C2 36 77 4A 48 73 2C 0C 58 70 38 F4 B9 DE 83 2B DA
           F4 D5 BF 0D 7C 88 E4 97 E1 3C 97 1F 9A A8 72 75 08 7D 9B 20
           C6 8B D5 1F 31 32 52 70 4D 89 F2 FA 2B FF 6C 83 BC 75 69 DC
           CC 14 5E 1A C9 7D 92 0F B6 97 BD AA 51 4C 2B C2 94 20 FD 48
           1F EA  [...]
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

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 10.0.2.15 to 10.0.2.8 :
10.0.2.15
10.0.2.8

Hop Count: 1
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2024/06/24

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

See Also

https://www.owasp.org/index.php/HttpOnly

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801

XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/8585/www

```
The following cookie does not set the HttpOnly cookie flag :

Name : nf_wp_session
Path : /wordpress/
Value : d532cfe87ad8f3b8085a1beace265f57%7C%7C1719450869%7C%7C1719450809
Domain :
Version : 1
Expires : Thu, 27-Jun-2024 01:14:29 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/8585/www

```
The following cookie does not set the secure cookie flag :

Name : nf_wp_session
Path : /wordpress/
Value : d532cfe87ad8f3b8085a1beace265f57%7C%7C1719450869%7C%7C1719450809
Domain :
Version : 1
Expires : Thu, 27-Jun-2024 01:14:29 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/8585/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://10.0.2.8:8585/
  - http://10.0.2.8:8585/index.php
  - http://10.0.2.8:8585/uploads/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/9l0UyBC3.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/9l0UyBC3.htm/RAoW4KDM.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/V9D9Bwzx.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/KHtOAs4H.htm/SFozlpWs.htm/
  - http://10.0.2.8:8585/uploads/1703xoR7.htm/QrcxOEde.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/2WdwFypX.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/LCUVhZ7z.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/R2Mqyy6X.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/T9vq7fVh.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/xzrVs9l0.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/R2WdwFyp.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/RRnHOMMz.htm/
```

```
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/YDxVuZ14.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/dWikEPIR.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/lXGguc6o.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/vs60_iuJ.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/QE2A2sKS.htm/
  - http://10.0.2.8:8585/uploads/1IXeyCeN.htm/4tWwXWQ0.htm/gJJ [...]
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

Plugin Output

tcp/8585/www

```
The following directories were discovered:
/cgi-bin, /uploads

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2024/05/20

Plugin Output

tcp/8585/www

```
Webmirror performed 139 queries in 3s (46.0333 queries per second)

The following CGIs have been discovered :


+ CGI : /index.php
  Methods : GET
  Argument : img
   Value: favicon


+ CGI : /
  Methods : GET
  Argument : lang
   Value: fr
  Argument : phpinfo
   Value: 1


+ CGI : /wordpress/
  Methods : GET
  Argument : s

Directory index found at /uploads/
Directory index found at /uploads/1IXeyCeN.htm/
Directory index found at /uploads/1pGNxzKT.htm/
Directory index found at /uploads/1703xoR7.htm/
```

```
Directory index found at /uploads/D0ldypfj.htm/
Directory index found at /uploads/LWEhweFS.htm/
Directory index found at /uploads/PiAlp2ys.htm/
Directory index found at /uploads/SSpfdUCe.htm/
Directory index found at /uploads/VpaMchxk.htm/
Directory index found at /uploads/bkgxzrVs.htm/
Directory index found at /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/
Directory index found at /uploads/1IXeyCeN.htm/Bq2yUggQ.htm/
Directory index found at /uploads/1IXeyCeN.htm/FAsPqijg.htm/
Directory index found at /uploads/1IXeyCeN.htm/FBcOuVVD.htm/
Directory index found at /uploads/1IXeyCeN.htm/Zt3xEQVC.htm/
Directory index found at /uploads/1IXeyCeN.htm/cRt1WXi1.htm/
Directory index found at /uploads/1IXeyCeN.htm/hJEFNNRS.htm/
Directory index found at /uploads/1IXeyCeN.htm/hOBnN7OK.htm/
Directory index found at /uploads/1703xoR7.htm/9l0UyBC3.htm/
Directory index found at /uploads/1703xoR7.htm/KHtOAs4H.htm/
Directory index found at /uploads/1703xoR7.htm/QrcxOEde.htm/
Directory index found at /uploads/LWEhweFS.htm/DtPz2nfB.htm/
Directory index found at /uploads/LWEhweFS.htm/TprR2GWG.htm/
Directory index found at /uploads/PiAlp2ys.htm/hoUtX91J.htm/
Directory index found at /uploads/VpaMchxk.htm/9mkjPmwE.htm/
Directory index found at /uploads/VpaMchxk.htm/UybKyCRw.htm/
Directory index found at /uploads/VpaMchxk.htm/ojyxD9gA.htm/
Directory index found at /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/
Directory index found at /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/JKgaOwpX.htm/
Directory index found at /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/QE2A2sKS [...]
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/8585/www

24004 - WebDAV Directory Enumeration

Synopsis

Several directories on the remote host are DAV-enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

Disable DAV support if you do not use it.

Risk Factor

None

Plugin Information

Published: 2007/01/11, Modified: 2011/03/14

Plugin Output

tcp/8585/www

```
The following directories are DAV enabled :
 - /uploads/1703xoR7.htm/9l0UyBC3.htm/RAoW4KDM.htm/
 - /uploads/1703xoR7.htm/KHtOAs4H.htm/
 - /uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/
 - /uploads/1703xoR7.htm/KHtOAs4H.htm/DW1lk2dB.htm/V9D9Bwzx.htm/
 - /uploads/1703xoR7.htm/KHtOAs4H.htm/SFozlpWs.htm/
 - /uploads/1703xoR7.htm/QrcxOEde.htm/
 - /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/LCUVhZ7z.htm/
 - /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/2WdwFypX.htm/
 - /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/9siH2gRV.htm/
 - /uploads/1IXeyCeN.htm/4tWwXWQ0.htm/
 - /uploads/1IXeyCeN.htm/
 - /uploads/1703xoR7.htm/9l0UyBC3.htm/
 - /uploads/1703xoR7.htm/
 - /uploads/
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 3 NetBIOS names have been gathered :

 METASPLOITABLE3  = Computer name
 WORKGROUP        = Workgroup / Domain name
 METASPLOITABLE3  = File Server Service

The remote host has the following MAC address on its adapter :

   08:00:27:41:0f:1c
```

18297 - WordPress Detection

Synopsis

The remote web server contains a blog application written in PHP.

Description

The remote host is running WordPress, a free blog application written in PHP with a MySQL back-end.

See Also

https://wordpress.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0747

Plugin Information

Published: 2005/05/18, Modified: 2023/05/24

Plugin Output

tcp/8585/www

```
URL     : http://10.0.2.8:8585/wordpress
Version : 4.6.1
```

101841 - WordPress Outdated Plugin Detection

Synopsis

The remote WordPress application has outdated plugins installed

Description

The WordPress application running on the remote host has outdated plugins installed.

See Also

https://wordpress.org/

Solution

Update the listed plugins through the administrative dashboard.

Risk Factor

None

Plugin Information

Published: 2017/07/20, Modified: 2024/06/05

Plugin Output

tcp/8585/www

```
The following plugins are outdated:
Plugin Name: Ninja Forms
Plugin Version: 2.9.42
Latest Version: 3.8.4

The following plugins' versions could not be verified:
Plugin Name: akismet
Latest Version: 5.3.2
```

101842 - WordPress Plugin Detection

Synopsis

The remote WordPress application has plugins installed

Description

The WordPress application running on the remote host has plugins installed.

See Also

https://wordpress.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/07/20, Modified: 2024/06/24

Plugin Output

tcp/8585/www

```
Wordpress Install : http://10.0.2.8:8585/wordpress
Plugin : Version
akismet : unknown
Ninja Forms : 2.9.42

Themes:
twentyfifteen
twentyfourteen
twentysixteen
```