W12D4 – Second Scan –-> Metasploitable

Report generated by Tenable Nessus™ Mon, 10 Feb 2025 04:26:34 CET

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

Epic-Metasploitable.epicode

30	73	113	16	149
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Sun Feb 9 23:41:15 2025
End time: Mon Feb 10 04:26:33 2025

Host Information

DNS Name: Epic-Metasploitable.epicode
Netbios Name: METASPLOITABLE
IP: 192.168.51.101
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

57603 - Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow

Synopsis

The remote web server is affected by a buffer overflow vulnerability.

Description

According to its self-reported banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.13. As such, it includes a bundled version of the Apache Portable Runtime (APR) library that contains a flaw in 'apr_palloc()' that could cause a heap overflow.

Note that the Apache HTTP server itself does not pass unsanitized, user-provided sizes to this function so it could only be triggered through some other application that uses it in a vulnerable way.

See Also

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

Solution

Upgrade to Apache 2.2.13 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

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

VPR Score

6.7

EPSS Score

0.1124

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	35949
CVE	CVE-2009-2412
XREF	CWE:189

Plugin Information

Published: 2012/01/19, Modified: 2018/06/29

Plugin Output

tcp/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.13
```

45004 - Apache 2.2.x < 2.2.15 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 2.2.15. It is, therefore, potentially affected by multiple vulnerabilities :

- A TLS renegotiation prefix injection attack is possible. (CVE-2009-3555)

- The 'mod_proxy_ajp' module returns the wrong status code if it encounters an error which causes the back-end server to be put into an error state. (CVE-2010-0408)

- The 'mod_isapi' attempts to unload the 'ISAPI.dll' when it encounters various error states which could leave call-backs in an undefined state. (CVE-2010-0425)

- A flaw in the core sub-request process code can lead to sensitive information from a request being handled by the wrong thread if a multi-threaded environment is used. (CVE-2010-0434)

- Added 'mod_reqtimeout' module to mitigate Slowloris attacks. (CVE-2007-6750)

See Also

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

https://bz.apache.org/bugzilla/show_bug.cgi?id=48359

https://archive.apache.org/dist/httpd/CHANGES_2.2.15

Solution

Upgrade to Apache version 2.2.15 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

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

VPR Score

9.0

EPSS Score

0.9713

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)

References

BID	21865
BID	36935
BID	38491
BID	38494
BID	38580
CVE	CVE-2007-6750
CVE	CVE-2009-3555
CVE	CVE-2010-0408
CVE	CVE-2010-0425
CVE	CVE-2010-0434
XREF	Secunia:38776
XREF	CWE:200
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2010/10/20, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.15
```

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

EPSS Score

0.4667

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/80/www

```
URL              : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
```

```
    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

EPSS Score

0.4667

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/80/www

```
Source            : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
```

```
    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

EPSS Score

0.1741

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

6.7

EPSS Score

0.0094

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

EPSS Score

0.0132

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

EPSS Score

0.0318

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

EPSS Score

0.01

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

EPSS Score

0.9651

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

EPSS Score

0.0114

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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/80/www

```
URL                                  : http://Epic-Metasploitable.epicode/
Installed version                    : 2.2.8
Security End of Life                 : July 11, 2017
Time since Security End of Life (Est.) : >= 7 years
```

70728 - Apache PHP-CGI Remote Code Execution

Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution.

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

Solution

Upgrade to PHP 5.3.13 / 5.4.3 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

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

VPR Score

9.0

EPSS Score

0.9569

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

CVE	CVE-2012-2311
CVE	CVE-2012-2335
CVE	CVE-2012-2336
XREF	CERT:520827
XREF	EDB-ID:29290
XREF	EDB-ID:29316
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

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

Plugin Information

Published: 2013/11/01, Modified: 2023/04/25

Plugin Output

tcp/80/www

```
Nessus was able to verify the issue exists using the following request :

------------------------------ snip ------------------------------
POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+
%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F
%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F
%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E
%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F
%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F
%65%6E%76%3D%30+%2D%6E HTTP/1.1
Host: Epic-Metasploitable.epicode
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 115
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, */*
<?php echo "Content-Type:text/html\r\n\r\n"; echo 'php_cgi_remote_code_execution-1739154185';
 system('id'); die; ?>
------------------------------ snip ------------------------------

This produced the following output :

------------------------------ snip ------------------------------
uid=33(www-data) gid=33(www-data) groups=33(www-data)
------------------------------ snip ------------------------------
```

171340 - Apache Tomcat SEoL (<= 5.5.x)

Synopsis

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

Description

According to its version, Apache Tomcat is less than or equal to 5.5.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://tomcat.apache.org/tomcat-55-eol.html

Solution

Upgrade to a version of Apache Tomcat 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: 2024/05/06

Plugin Output

tcp/8180/www

```
URL                                  : http://Epic-Metasploitable.epicode:8180/
Installed version                    : 5.5
Security End of Life                 : September 30, 2012
Time since Security End of Life (Est.) : >= 12 years
```

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.2056

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)

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.2056

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)

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

tcp/25/smtp

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.2056

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)

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

tcp/5432/postgresql

94403 - Default Password 'service' for 'service' Account

Synopsis

An administrative account on the remote host uses a known default password.

Description

The account 'service' on the remote host has the default password 'service'. A remote attacker can exploit this issue to gain administrative access to the affected system.

Solution

Change the password for this account or disable it.

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

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

VPR Score

7.4

EPSS Score

0.013

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

CVE	CVE-1999-0502

Exploitable With

Metasploit (true)

Plugin Information

Published: 2016/10/28, Modified: 2022/04/11

Plugin Output

tcp/22/ssh

```
It was possible to execute the command 'id' on the remote host :

  uid=1002(service) gid=1002(service) groups=1002(service)
```

86072 - ISC BIND Unsupported Version Detection

Synopsis

The remote host is running an unsupported version of ISC BIND.

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is 9.8.x or earlier. It is, therefore, 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.

Solution

Upgrade to a version of ISC BIND that is currently supported.

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 v2.0 Base Score

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

References

XREF	IAVA:0001-A-0541

Plugin Information

Published: 2015/09/22, Modified: 2021/02/16

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11, 9.16, 9.17 or higher
End of Support URL: https://www.isc.org/downloads/
```

57558 - MySQL Unsupported Version Detection

Synopsis

The remote host is running an unsupported version of a database server.

Description

According to its version, the installation of MySQL 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

https://www.mysql.com/support/supportedplatforms/database.html

https://www.mysql.com/support/eol-notice.html

Solution

Upgrade to a version of MySQL that is currently supported.

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 v2.0 Base Score

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

References

XREF IAVA:0001-A-0567

Plugin Information

Published: 2012/01/16, Modified: 2024/09/09

Plugin Output

tcp/3306/mysql

```
Installed version   : 5.0.51a-3ubuntu5
Supported versions  : 8.0(LTS) / 8.4(LTS) / 9.0 or later versions.
```

```
   End of support date : January 9, 2012
```

90022 - OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security Bypass

Synopsis

The SSH server running on the remote host is affected by a security bypass vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.2. It is, therefore, affected by a security bypass vulnerability due to a flaw in ssh(1) that is triggered when it falls back from untrusted X11 forwarding to trusted forwarding when the SECURITY extension is disabled by the X server. This can result in untrusted X11 connections that can be exploited by a remote attacker.

See Also

http://www.openssh.com/txt/release-7.2

Solution

Upgrade to OpenSSH version 7.2 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

EPSS Score

0.0078

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

CVE CVE-2016-1908

Plugin Information

Published: 2016/03/18, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 7.2
```

178910 - OpenSSH < 9.3p2 Vulnerability

Synopsis

The SSH server running on the remote host is affected by a vulnerability.

Description

The version of OpenSSH installed on the remote host is prior to 9.3p2. It is, therefore, affected by a vulnerability as referenced in the release-9.3p2 advisory.

- Fix CVE-2023-38408 - a condition where specific libaries loaded via ssh-agent(1)'s PKCS#11 support could be abused to achieve remote code execution via a forwarded agent socket if the following (openssh-9.3p2-1)

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://www.openssh.com/txt/release-9.3p2

Solution

Upgrade to OpenSSH 9.3p2 / 9.4 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

EPSS Score

0.0399

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)

References

CVE CVE-2023-38408

Plugin Information

Published: 2023/07/26, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 9.3p2 / 9.4
```

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: 2024/11/22

Plugin Output

tcp/80/www

```
  Source              : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
```

```
   Installed version   : 5.2.4-2ubuntu5.10
   End of support date : 2011/01/06
   Announcement        : http://php.net/eol.php
   Supported versions  : 8.1.x / 8.2.x / 8.3.x
```

63347 - PostgreSQL Unsupported Version Detection

Synopsis

The remote host is running an unsupported version of a database server.

Description

According to its self-reported version number, the installation of PostgreSQL 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

https://www.postgresql.org/support/versioning/

Solution

Upgrade to a version of PostgreSQL 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-0583

Plugin Information

Published: 2012/12/28, Modified: 2025/02/05

Plugin Output

tcp/5432/postgresql

```
Version source     : Fauth.c.L1003.Rauth_failed
Installed version  : 8.3.8
```

```
  Supported versions : 9.6 / 10 / 11 / 12 / 13
```

50544 - ProFTPD < 1.3.3c Multiple Vulnerabilities

Synopsis

The remote FTP server is affected by multiple vulnerabilities.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

According to its banner, the version of ProFTPD installed on the remote host is earlier than 1.3.3c. Such versions are reportedly affected by the following vulnerabilities :

- When ProFTPD is compiled with 'mod_site_misc' and a directory is writable, a user can use 'mod_site_misc' to create or delete a directory outside the writable directory, create a symlink located outside the writable directory, or change the time of a file located outside the writable directory. (Bug #3519)

- A stack-based buffer overflow exists in the server's 'pr_netio_telnet_gets()' function, which can be triggered by when reading user input containing a TELNET_IAC escape sequence. (Bug #3521)

Note that Nessus did not actually test for the flaws but instead has relied on the version in ProFTPD's banner so this may be a false positive.

See Also

http://www.zerodayinitiative.com/advisories/ZDI-10-229/

http://bugs.proftpd.org/show_bug.cgi?id=3519

http://bugs.proftpd.org/show_bug.cgi?id=3521

http://www.nessus.org/u?c2cebd53

Solution

Upgrade to ProFTPD version 1.3.3c or later.

Risk Factor

Critical

VPR Score

7.4

EPSS Score

0.8334

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)

References

BID	44562
CVE	CVE-2010-3867
CVE	CVE-2010-4221
XREF	EDB-ID:15449
XREF	Secunia:42052

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2010/11/10, Modified: 2020/03/27

Plugin Output

tcp/2121/ftp

```
  Version source    : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
500 GET not understood
  Installed version : 1.3.1
  Fixed version     : 1.3.3c
```

58662 - Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows

Synopsis

The remote Samba server is affected by multiple buffer overflow vulnerabilities.

Description

According to its banner, the version of Samba 3.x running on the remote host is earlier than 3.6.4 / 3.5.14 / 3.4.16. It is, therefore, affected by multiple heap-based buffer overflow vulnerabilities.

An error in the DCE/RPC IDL (PIDL) compiler causes the RPC handling code it generates to contain multiple heap-based buffer overflow vulnerabilities. This generated code can allow a remote, unauthenticated attacker to use malicious RPC calls to crash the application and possibly execute arbitrary code as the root user.

Note that Nessus has not actually tried to exploit this issue or otherwise determine if one of the associated patches has been applied.

See Also

https://www.zerodayinitiative.com/advisories/ZDI-12-061/

https://www.zerodayinitiative.com/advisories/ZDI-12-062/

https://www.zerodayinitiative.com/advisories/ZDI-12-063/

https://www.zerodayinitiative.com/advisories/ZDI-12-064/

https://www.zerodayinitiative.com/advisories/ZDI-12-068/

https://www.zerodayinitiative.com/advisories/ZDI-12-069/

https://www.zerodayinitiative.com/advisories/ZDI-12-070/

https://www.zerodayinitiative.com/advisories/ZDI-12-071/

https://www.zerodayinitiative.com/advisories/ZDI-12-072/

https://www.samba.org/samba/security/CVE-2012-1182.html

https://www.samba.org/samba/history/samba-3.6.4.html

https://www.samba.org/samba/history/samba-3.5.14.html

https://www.samba.org/samba/history/samba-3.4.16.html

https://www.samba.org/samba/history/security.html

Solution

Either install the appropriate patch referenced in the project's advisory or upgrade to 3.6.4 / 3.5.14 / 3.4.16 or later.

Risk Factor

Critical

VPR Score

7.4

EPSS Score

0.881

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)

References

BID	52973
CVE	CVE-2012-1182
XREF	ZDI:ZDI-12-061
XREF	ZDI:ZDI-12-062
XREF	ZDI:ZDI-12-063
XREF	ZDI:ZDI-12-064
XREF	ZDI:ZDI-12-068
XREF	ZDI:ZDI-12-069
XREF	ZDI:ZDI-12-070
XREF	ZDI:ZDI-12-071
XREF	ZDI:ZDI-12-072

Exploitable With

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

Plugin Information

Published: 2012/04/11, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Installed version  : 3.0.20-Debian
Fixed version      : 3.6.4 / 3.5.14 / 3.4.16
```

25217 - Samba < 3.0.25 Multiple Vulnerabilities

Synopsis

The remote Samba server is affected by multiple vulnerabilities.

Description

According to its banner, the version of the Samba server installed on the remote host is affected by multiple buffer overflow and remote command injection vulnerabilities, which can be exploited remotely, as well as a local privilege escalation bug.

See Also

http://www.samba.org/samba/security/CVE-2007-2444.html

http://www.samba.org/samba/security/CVE-2007-2446.html

http://www.samba.org/samba/security/CVE-2007-2447.html

Solution

Upgrade to Samba version 3.0.25 or later.

Risk Factor

Critical

VPR Score

7.4

EPSS Score

0.9359

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)

References

BID	23972
BID	23973
BID	23974

BID	24195
BID	24196
BID	24197
BID	24198
CVE	CVE-2007-2444
CVE	CVE-2007-2446
CVE	CVE-2007-2447

Exploitable With

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

Plugin Information

Published: 2007/05/15, Modified: 2018/07/27

Plugin Output

tcp/445/cifs

169505 - Samba < 4.15.13 / 4.16.x < 4.16.8 / 4.17.x < 4.17.4 Multiple Vulnerabilities

Synopsis

The remote Samba server is potentially affected by multiple vulnerabilities.

Description

The version of Samba running on the remote host is prior to 4.15.13, 4.16.x prior to 4.16.8, or 4.17.x prior to 4.17.4. It is, therefore, affected by multiple vulnerabilities:

- Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability. (CVE-2022-37966, CVE-2022-45141)

- Windows Kerberos Elevation of Privilege Vulnerability. (CVE-2022-37967)

- Netlogon RPC Elevation of Privilege Vulnerability. (CVE-2022-38023)

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.samba.org/samba/history/security.html

https://www.samba.org/samba/security/CVE-2022-38023.html

https://www.samba.org/samba/security/CVE-2022-37966.html

https://www.samba.org/samba/security/CVE-2022-37967.html

https://www.samba.org/samba/security/CVE-2022-45141.html

Solution

Upgrade to Samba version 4.15.13, 4.16.8, or 4.17.4 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

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

VPR Score

7.4

EPSS Score

0.0185

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

CVE	CVE-2022-37966
CVE	CVE-2022-37967
CVE	CVE-2022-38023
CVE	CVE-2022-45141
XREF	IAVA:2023-A-0004-S

Plugin Information

Published: 2023/01/04, Modified: 2023/09/11

Plugin Output

tcp/445/cifs

```
Installed version : 3.0.20-Debian
Fixed version     : 4.15.13
```

76314 - Samba Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of Samba.

Description

According to its self-reported version number, the installation of Samba 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

https://wiki.samba.org/index.php/Samba_Release_Planning

Solution

Upgrade to a version of Samba 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-0593

Plugin Information

Published: 2014/06/30, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
Installed version : 3.0.20-Debian
EOL date          : 2009/08/05
```

```
   EOL URL           : https://wiki.samba.org/index.php/Samba_Release_Planning
   Supported version : 4.6.x / 4.7.x / 4.8.x
```

125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

Synopsis

The remote web server hosts a PHP application that is affected by SQLi vulnerability.

Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.

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

See Also

http://www.nessus.org/u?c9d7fc8c

Solution

Upgrade to phpMyAdmin version 4.8.6 or later.

Alternatively, apply the patches referenced in the vendor advisories.

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

EPSS Score

0.0081

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	108617
CVE	CVE-2019-11768

Plugin Information

Published: 2019/06/13, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
URL               : http://Epic-Metasploitable.epicode/phpMyAdmin
Installed version : 3.1.1
Fixed version     : 4.8.6
```

40467 - Apache 2.2.x < 2.2.12 Multiple Vulnerabilities

Synopsis

The remote web server may be affected by several issues.

Description

According to its banner, the version of Apache 2.2.x. running on the remote host is prior to 2.2.12. It is, therefore, affected by the following vulnerabilities :

- A heap-based buffer underwrite flaw exists in the function 'apr_strmatch_precompile()' in the bundled copy of the APR-util library, which could be triggered when parsing configuration data to crash the daemon.

(CVE-2009-0023)

- A flaw in the mod_proxy_ajp module in version 2.2.11 only may allow a remote attacker to obtain sensitive response data intended for a client that sent an earlier POST request with no request body.

(CVE-2009-1191)

- The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195)

- Failure to properly handle an amount of streamed data that exceeds the Content-Length value allows a remote attacker to force a proxy process to consume CPU time indefinitely when mod_proxy is used in a reverse proxy configuration. (CVE-2009-1890)

- Failure of mod_deflate to stop compressing a file when the associated network connection is closed may allow a remote attacker to consume large amounts of CPU if there is a large (>10 MB) file available that has mod_deflate enabled. (CVE-2009-1891)

- Using a specially crafted XML document with a large number of nested entities, a remote attacker may be able to consume an excessive amount of memory due to a flaw in the bundled expat XML parser used by the mod_dav and mod_dav_svn modules. (CVE-2009-1955)

- There is an off-by-one overflow in the function 'apr_brigade_vprintf()' in the bundled copy of the APR-util library in the way it handles a variable list of arguments, which could be leveraged on big-endian platforms to perform information disclosure or denial of service attacks. (CVE-2009-1956)

Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use.

See Also

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

Solution

Upgrade to Apache version 2.2.12 or later. Alternatively, ensure that the affected modules / directives are not in use.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.4

EPSS Score

0.358

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

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

References

BID	34663
BID	35115
BID	35221
BID	35251
BID	35253
BID	35565
BID	35623
CVE	CVE-2009-0023
CVE	CVE-2009-1191
CVE	CVE-2009-1195
CVE	CVE-2009-1890
CVE	CVE-2009-1891
CVE	CVE-2009-1955
CVE	CVE-2009-1956
XREF	CWE:16
XREF	CWE:20
XREF	CWE:119
XREF	CWE:189
XREF	CWE:399

Plugin Information

Published: 2009/08/02, Modified: 2020/04/27

Plugin Output

tcp/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.12
```

42052 - Apache 2.2.x < 2.2.14 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 2.2.14. It is, therefore, potentially affected by multiple vulnerabilities :

- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)

- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)

- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial of service. (CVE-2009-3094)

Note that the remote web server may not actually be affected by these vulnerabilities as Nessus did not try to determine whether the affected modules are in use or check for the issues themselves.

See Also

http://www.securityfocus.com/advisories/17947

http://www.securityfocus.com/advisories/17959

http://www.nessus.org/u?e470f137

https://bz.apache.org/bugzilla/show_bug.cgi?id=47645

http://www.nessus.org/u?c34c4eda

Solution

Upgrade to Apache version 2.2.14 or later. Alternatively, ensure that the affected modules are not in use.

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

6.7

EPSS Score

0.499

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	36254
BID	36260
BID	36596
CVE	CVE-2009-2699
CVE	CVE-2009-3094
CVE	CVE-2009-3095
XREF	Secunia:36549
XREF	CWE:119
XREF	CWE:264

Plugin Information

Published: 2009/10/07, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.14
```

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

EPSS Score

0.0038

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/80/www

```
  Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
  Installed version : 2.2.8
  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

EPSS Score

0.9575

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/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.29
```

96450 - Apache 2.2.x < 2.2.32 Multiple Vulnerabilities (httpoxy)

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 2.2.32. It is, therefore, affected by the following vulnerabilities :

- The Apache HTTP Server is affected by a man-in-the-middle vulnerability known as 'httpoxy' due to a failure to properly resolve namespace conflicts in accordance with RFC 3875 section 4.1.18. The HTTP_PROXY environment variable is set based on untrusted user data in the 'Proxy' header of HTTP requests. The HTTP_PROXY environment variable is used by some web client libraries to specify a remote proxy server. An unauthenticated, remote attacker can exploit this, via a crafted 'Proxy' header in an HTTP request, to redirect an application's internal HTTP traffic to an arbitrary proxy server where it may be observed or manipulated.

(CVE-2016-5387)

- A flaw exists due to improper handling of whitespace patterns in user-agent headers. An unauthenticated, remote attacker can exploit this, via a specially crafted user-agent header, to cause the program to incorrectly process sequences of requests, resulting in interpreting responses incorrectly, polluting the cache, or disclosing the content from one request to a second downstream user-agent. (CVE-2016-8743)

- A CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir (CVE-2016-4975)

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/dev/dist/Announcement2.2.html

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

https://github.com/apache/httpd/blob/2.2.x/CHANGES

https://www.apache.org/security/asf-httpoxy-response.txt

https://httpoxy.org

Solution

Upgrade to Apache version 2.2.32 or later.

Note that the 'httpoxy' vulnerability can be mitigated by applying the workarounds or patches as referenced in the vendor advisory asf-httpoxy-response.txt.

Risk Factor

Medium

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

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

VPR Score

6.7

EPSS Score

0.5563

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	91816
BID	95077
BID	105093
CVE	CVE-2016-4975
CVE	CVE-2016-5387
CVE	CVE-2016-8743
XREF	CERT:797896

Plugin Information

Published: 2017/01/12, Modified: 2019/03/27

Plugin Output

tcp/80/www

```
Source            : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.32
```

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

EPSS Score

0.004

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

EPSS Score

0.1578

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

EPSS Score

0.02

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

EPSS Score

0.0013

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

3.6

EPSS Score

0.0574

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
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

4.4

EPSS Score

0.0019

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-S

Plugin Information

Published: 2024/04/04, Modified: 2024/07/12

Plugin Output

tcp/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
Fixed version     : 2.4.59
```

55976 - Apache HTTP Server Byte Range DoS

Synopsis

The web server running on the remote host is affected by a denial of service vulnerability.

Description

The version of Apache HTTP Server running on the remote host is affected by a denial of service vulnerability. Making a series of HTTP requests with overlapping ranges in the Range or Request-Range request headers can result in memory and CPU exhaustion. A remote, unauthenticated attacker could exploit this to make the system unresponsive.

Exploit code is publicly available and attacks have reportedly been observed in the wild.

See Also

https://seclists.org/fulldisclosure/2011/Aug/175

https://lists.gt.net/apache/dev/401638

http://www.nessus.org/u?404627ec

http://httpd.apache.org/security/CVE-2011-3192.txt

http://www.nessus.org/u?213307e6

http://www-01.ibm.com/support/docview.wss?uid=swg24030863

Solution

Upgrade to Apache httpd 2.2.21 or later. Alternatively, apply one of the workarounds in Apache's advisories for CVE-2011-3192. Version 2.2.20 fixed the issue, but it also introduced a regression.

If the host is running a web server based on Apache httpd, contact the vendor for a fix.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.6

EPSS Score

0.9696

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

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

References

BID	49303
CVE	CVE-2011-3192
XREF	CERT:405811
XREF	EDB-ID:17696
XREF	EDB-ID:18221

Exploitable With

Core Impact (true)

Plugin Information

Published: 2011/08/25, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Nessus determined the server is unpatched and is not using any
of the suggested workarounds by making the following requests :

-------------------- Testing for workarounds --------------------
HEAD /mutillidae/framer.html HTTP/1.1
Host: Epic-Metasploitable.epicode
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Request-Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
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, */*
HTTP/1.1 206 Partial Content
Date: Mon, 10 Feb 2025 02:58:36 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Last-Modified: Thu, 12 Jan 2012 00:51:50 GMT
ETag: "164e4-59d-4b64a274c7580"
Accept-Ranges: bytes
Content-Length: 847
Keep-Alive: timeout=15, max=100
```

```
Connection: Keep-Alive
Content-Type: multipart/x-byteranges; boundary=62dc0e2709b015f95
-------------------- Testing for workarounds --------------------

-------------------- Testing for patch --------------------
HEAD /mutillidae/framer.html HTTP/1.1
Host: Epic-Metasploitable.epicode
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Request-Range: bytes=0-,1-
Range: bytes=0-,1-
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, */*
HTTP/1.1 206 Partial Content
Date: Mon, 10 Feb 2025 02:58:51 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Last-Modified: Thu, 12 Jan 2012 00:51:50 GMT
ETag: "164e4-59d-4b64a274c7580"
Accept-Ranges: bytes
Content-Length: 3066
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: multipart/x-byteranges; boundary=62dc0e35571b91453
-------------------- Testing for patch --------------------
```

39465 - CGI Generic Command Execution

Synopsis

Arbitrary code may be run on the remote server.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to execute arbitrary commands on the remote host.

See Also

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

http://projects.webappsec.org/w/page/13246950/OS%20Commanding

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address command execution flaws.

Risk Factor

High

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:77
XREF	CWE:78
XREF	CWE:713
XREF	CWE:722
XREF	CWE:727
XREF	CWE:741
XREF	CWE:751
XREF	CWE:801
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/06/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to arbitrary command execution :

+ The 'topic' parameter of the /twiki/bin/view/Main/WebHome CGI :

/twiki/bin/view/Main/WebHome?topic=echo%20NeS%20%20SuS

-------- output --------
<body bgcolor="#ffffff">
<a name="PageTop"></a>
<form name="main" action="/twiki/bin/view/Main/echo%20NeS%20SuS">
<table width="100%" border="0" cellpadding="3" cellspacing="0">
<tr>
------------------------
```

39469 - CGI Generic Remote File Inclusion

Synopsis

Arbitrary code may be run on the remote server.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.

See Also

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

http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

Risk Factor

High

CVSS v2.0 Base Score

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

References

XREF	CWE:73
XREF	CWE:78
XREF	CWE:98
XREF	CWE:434
XREF	CWE:473
XREF	CWE:632
XREF	CWE:714
XREF	CWE:727
XREF	CWE:801
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to web code injection :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=http://IXsOkvVR.example.com/

-------- output --------
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>:  include(http://IXsOkvVR.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/mutillidae/index.php</b> on line <b>4
69</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------

+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?page=http://IXsOkvVR.example.com/

-------- output --------
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>:  include(http://IXsOkvVR.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/mutillidae/index.php</b> on line <b>4
69</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------


Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to web code injection :

/mutillidae/index.php [do=toggle-hints&page=http://IXsOkvVR.example.com/
&username=anonymous]

-------- output --------
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>:  include(http://IXsOkvVR.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/mutillidae/index.php</b> on line <b>4
69</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------
```

42424 - CGI Generic SQL Injection (blind)

Synopsis

A CGI application hosted on the remote web server is potentially prone to SQL injection attack.

Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

See Also

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

http://www.nessus.org/u?ed792cf5

http://www.nessus.org/u?11ab1866

Solution

Modify the affected CGI scripts so that they properly escape arguments.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:77
XREF	CWE:89
XREF	CWE:91
XREF	CWE:203
XREF	CWE:643
XREF	CWE:713
XREF	CWE:722

XREF	CWE:727
XREF	CWE:751
XREF	CWE:801
XREF	CWE:810
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/11/06, Modified: 2024/06/14

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to blind SQL injection :

+ The 'do' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?username=anonymous&page=home.php&do=toggle-hintszz
anonymous&page=home.php&do=toggle-hintsyy

-------- output --------
HTTP/1.1 302 Found
-------- vs --------
HTTP/1.1 200 OK
------------------------


Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to blind SQL injection :

+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php [username=anonymous&do=toggle-hints&page=home.phpz
zanonymous&do=toggle-hints&page=home.phpyy]

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=home.php">Toggle Hint
s</a></td><td><a href="./index.php?do=toggle-security&page=home.php
">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
-------- vs --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=home.phpyy">Toggle Hi
nts</a></td><td><a href="./index.php?do=toggle-security&page=home.p
hpyy">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

/mutillidae/index.php [username=anonymous&do=toggle-hints&page=home.phpz
zanonymous&do=toggle-hints&page=home.phpyy] {2}
```

```
-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=home.php">Toggle Hint
s</a></td><td><a href="./index.php?do=toggle-security&page=home.php
">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
-------- vs -- [...]
```

96625 - ISC BIND 9 < 9.9.9-P5 / 9.9.9-S7 / 9.10.4-P5 / 9.11.0-P2 Multiple DoS

Synopsis

The remote name server is affected by multiple denial of service vulnerabilities.

Description

According to its self-reported version number, the instance of ISC BIND 9 running on the remote name server is 9.9.x prior to 9.9.9-P5 or 9.9.9-S7, 9.10.x prior to 9.10.4-P5, or 9.11.x prior to 9.11.0-P2. It is, therefore, affected by multiple denial of service vulnerabilities :

- A denial of service vulnerability exists in named due to a flaw that is triggered during the handling of a specially crafted answer packet in a response to an RTYPE ANY query. An unauthenticated, remote attacker can exploit this to cause an assertion failure and daemon exit. Note that this vulnerability affects versions 9.4.0 to 9.6-ESV-R11-W1, 9.8.5 to 9.8.8, 9.9.3 to 9.9.9-P4, 9.9.9-S1 to 9.9.9-S6, 9.10.0 to 9.10.4-P4, and 9.11.0 to 9.11.0-P1. (CVE-2016-9131)

- A denial of service vulnerability exists in named in DNSSEC-enabled authoritative servers that is triggered during the handling of a query response that contains inconsistent DNSSEC information. An unauthenticated, remote attacker can exploit this to cause an assertion failure and daemon exit. Note that this vulnerability affects versions 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, and 9.11.0-P1. (CVE-2016-9147)

- A denial of service vulnerability exists in named due to a flaw that is triggered during the handling of a specially crafted answer that contains a DS resource record. An unauthenticated, remote attacker can exploit this to cause an assertion failure and daemon exit. Note that this vulnerability affects versions 9.6-ESV-R9 to 9.6-ESV-R11-W1, 9.8.5 to 9.8.8, 9.9.3 to 9.9.9-P4, 9.9.9-S1 to 9.9.9-S6, 9.10.0 to 9.10.4-P4, and 9.11.0 to 9.11.0-P1. (CVE-2016-9444)

- A denial of service vulnerability exists in named in the nxdomain-redirect functionality that is triggered when handling a specially crafted query. An unauthenticated, remote attacker can exploit this to cause a REQUIRE assertion failure and daemon exit. Note that this vulnerability affects versions 9.9.8-S1 to 9.9.8-S3, 9.9.9-S1 to 9.9.9-S6, and 9.11.0-9.11.0 to P1.

(CVE-2016-9778)

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://kb.isc.org/article/AA-01439

https://kb.isc.org/article/AA-01440

https://kb.isc.org/article/AA-01441

https://kb.isc.org/docs/aa-01442

Solution

Upgrade to ISC BIND version 9.9.9-P5 / 9.9.9-S7 / 9.10.4-P5 / 9.11.0-P2 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

EPSS Score

0.7753

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	95386
BID	95388
BID	95390
BID	95393
CVE	CVE-2016-9131
CVE	CVE-2016-9147
CVE	CVE-2016-9444
CVE	CVE-2016-9778

Plugin Information

Published: 2017/01/19, Modified: 2018/12/07

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.9-P5 / 9.9.9-S7 / 9.10.4-P5 / 9.11.0-P2
```

62562 - ISC BIND 9 DNS RDATA Handling DoS

Synopsis

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

Description

According to its self-reported version number, the remote installation of BIND can become locked up if certain combinations of RDATA are loaded into the server. Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

See Also

https://kb.isc.org/docs/aa-00801

http://ftp.isc.org/isc/bind9/9.6-ESV-R7-P4/CHANGES

http://ftp.isc.org/isc/bind9/9.7.6-P4/CHANGES

http://ftp.isc.org/isc/bind9/9.8.3-P4/CHANGES

http://ftp.isc.org/isc/bind9/9.9.1-P4/CHANGES

Solution

Upgrade to BIND 9.6-ESV-R7-P4 / 9.6-ESV-R8 / 9.7.6-P4 / 9.7.7 / 9.8.3-P4 / 9.8.4 / 9.9.1-P4 / 9.9.2 or later.

Risk Factor

High

VPR Score

3.6

EPSS Score

0.1022

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)

References

BID	55852

CVE CVE-2012-5166

Plugin Information

Published: 2012/10/16, Modified: 2018/11/15

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.6-ESV-R7-P4
```

60120 - ISC BIND 9 Multiple Denial of Service Vulnerabilities

Synopsis

The remote name server may be affected by multiple denial of service vulnerabilities.

Description

According to its self-reported version number, the remote installation of BIND is affected by multiple denial of service vulnerabilities :

- Under a heavy query load, the application may use uninitialized data structures related to failed query cache access. This error can cause the application to crash. Note this issue only affects the application when DNSSEC validation is enabled. (CVE-2012-3817)

- Under a heavy, incoming TCP query load, the application can be affected by a memory leak that can lead to decreased performance and application termination on systems that kill processes that are out of memory.

(CVE-2012-3868)

Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

See Also

https://kb.isc.org/article/AA-00729

https://kb.isc.org/docs/aa-00730

http://ftp.isc.org/isc/bind9/9.6-ESV-R7-P2/CHANGES

http://ftp.isc.org/isc/bind9/9.7.6-P2/CHANGES

http://ftp.isc.org/isc/bind9/9.8.3-P2/CHANGES

http://ftp.isc.org/isc/bind9/9.9.1-P2/CHANGES

Solution

Upgrade to BIND 9.6-ESV-R7-P2 / 9.7.6-P2 / 9.8.3-P2 / 9.9.1-P2 or later.

Risk Factor

High

VPR Score

3.6

EPSS Score

0.0949

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)

References

BID	54658
BID	54659
CVE	CVE-2012-3817
CVE	CVE-2012-3868

Plugin Information

Published: 2012/07/25, Modified: 2018/11/15

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.6-ESV-R7-P2
```

89999 - ISC BIND 9 Multiple DoS

Synopsis

The remote name server is affected by multiple denial of service vulnerabilities.

Description

According to its self-reported version number, the instance of ISC BIND running on the remote name server is affected by multiple denial of service vulnerabilities :

- A denial of service vulnerability exists in files resolver.c and db.c when handling DNAME resource signatures. An unauthenticated, remote attacker can exploit this, via a crafted query that generates a response containing a signature record, to cause an assertion failure and daemon exit. (CVE-2016-1286)

- A denial of service vulnerability exists in resolver.c when DNS cookies are enabled. An unauthenticated, remote attacker can exploit this, via a malformed cookie with more than one cookie option, to cause an INSIST assertion failure and daemon exit. (CVE-2016-2088)

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://kb.isc.org/docs/aa-01353

https://kb.isc.org/article/AA-01362/

Solution

Upgrade to ISC BIND version 9.9.8-P4 / 9.9.8-S6 / 9.10.3-P4 or later.

Note that version 9.9.8-S6 is a preview version of BIND provided exclusively to ISC Support customers. Additionally, the fix for CVE-2016-2088 is only available in version 9.10.3-P4.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.8396

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

CVE	CVE-2016-1286
CVE	CVE-2016-2088

Plugin Information

Published: 2016/03/17, Modified: 2019/11/20

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.8-P4 / 9.9.8-S6 / 9.10.3-P4
```

79861 - ISC BIND 9 Multiple DoS Vulnerabilities

Synopsis

The remote name server is affected by multiple denial of service vulnerabilities.

Description

According to its self-reported version number, the remote installation of BIND is affected by multiple denial of service vulnerabilities :

- A flaw exists within the Domain Name Service due to an error in the code used to follow delegations. A remote attacker, with a maliciously-constructed zone or query, could potentially cause the service to issue unlimited queries leading to resource exhaustion. (CVE-2014-8500)

- Multiple flaws exist with the GeoIP feature. These flaws could allow a remote attacker to cause a denial of service. Note these issues only affect the 9.10.x branch. (CVE-2014-8680)

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://kb.isc.org/docs/aa-01216

https://kb.isc.org/docs/aa-01217

http://www.nessus.org/u?92718697

http://www.nessus.org/u?9f54d158

Solution

Upgrade to BIND version 9.9.6-P1 / 9.10.1-P1 or later.

Risk Factor

High

VPR Score

3.6

EPSS Score

0.7196

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)

References

BID	71590
BID	73191
CVE	CVE-2014-8500
CVE	CVE-2014-8680

Plugin Information

Published: 2014/12/12, Modified: 2018/11/15

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.6-P1
```

94577 - ISC BIND 9 Recursive Response DNAME Record Handling DoS

Synopsis

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

Description

According to its self-reported version number, the instance of ISC BIND 9 running on the remote name server is affected by a denial of service vulnerability due to improper handling of a recursive response containing a DNAME record in the answer section. An unauthenticated, remote attacker can exploit this to cause an assertion failure and daemon exit.

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://kb.isc.org/article/AA-01434/

Solution

Upgrade to ISC BIND version 9.9.9-P4 / 9.9.9-S6 / 9.10.4-P4 / 9.11.0-P1 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

EPSS Score

0.9292

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	94067
CVE	CVE-2016-8864

Plugin Information

Published: 2016/11/04, Modified: 2018/12/07

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.9-P4 / 9.9.9-S6 / 9.10.4-P4 / 9.11.0-P1
```

59446 - ISC BIND 9 Zero-Length RDATA Section Denial of Service / Information Disclosure

Synopsis

The remote name server may be affected by a denial of service / information disclosure vulnerability.

Description

According to its self-reported version number, the remote installation of BIND does not properly handle resource records with a zero-length RDATA section, which may lead to unexpected outcomes, such as crashes of the affected server, disclosure of portions of memory, corrupted zone data, or other problems.

Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

See Also

http://ftp.isc.org/isc/bind9/9.6-ESV-R7-P1/CHANGES

http://ftp.isc.org/isc/bind9/9.7.6-P1/CHANGES

http://ftp.isc.org/isc/bind9/9.8.3-P1/CHANGES

http://ftp.isc.org/isc/bind9/9.9.1-P1/CHANGES

https://kb.isc.org/docs/aa-00698

https://www.isc.org/software/bind/advisories/cve-2012-1667

Solution

Upgrade to BIND 9.6-ESV-R7-P1 / 9.7.6-P1 / 9.8.3-P1 / 9.9.1-P1 or later.

Risk Factor

High

VPR Score

3.6

EPSS Score

0.9038

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	53772
CVE	CVE-2012-1667
XREF	CERT:381699

Plugin Information

Published: 2012/06/11, Modified: 2018/11/15

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.6-ESV-R7-P1
```

190444 - ISC BIND 9.0.0 < 9.16.48 / 9.9.3-S1 < 9.16.48-S1 / 9.18.0 < 9.18.24 / 9.18.11-S1 < 9.18.24-S1 / 9.19.0 < 9.19.21 Vulnerability (cve-2023-50387)

Synopsis

The remote name server is affected by a vulnerability vulnerability.

Description

The version of ISC BIND installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the cve-2023-50387 advisory.

- Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the KeyTrap issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records. (CVE-2023-50387)

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://kb.isc.org/v1/docs/cve-2023-50387

Solution

Upgrade to ISC BIND version 9.16.48 / 9.16.48-S1 / 9.18.24 / 9.18.24-S1 / 9.19.21 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

5.1

EPSS Score

0.0465

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-2023-50387
XREF	IAVA:2024-A-0103-S

Plugin Information

Published: 2024/02/13, Modified: 2024/07/26

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.16.48
```

190462 - ISC BIND 9.0.0 < 9.16.48 / 9.9.3-S1 < 9.16.48-S1 / 9.18.0 < 9.18.24 / 9.18.11-S1 < 9.18.24-S1 / 9.19.0 < 9.19.21 Vulnerability (cve-2023-50868)

Synopsis

The remote name server is affected by a vulnerability vulnerability.

Description

The version of ISC BIND installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the cve-2023-50868 advisory.

- The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the NSEC3 issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations. (CVE-2023-50868)

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://kb.isc.org/v1/docs/cve-2023-50868

Solution

Upgrade to ISC BIND version 9.16.48 / 9.16.48-S1 / 9.18.24 / 9.18.24-S1 / 9.19.21 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

EPSS Score

0.0005

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-2023-50868
XREF	IAVA:2024-A-0103-S

Plugin Information

Published: 2024/02/13, Modified: 2024/07/26

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.16.48
```

85896 - ISC BIND 9.0.x < 9.9.7-P3 / 9.10.x < 9.10.2-P4 Multiple DoS

Synopsis

The remote name server is affected by multiple denial of service vulnerabilities.

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is potentially affected by the following vulnerabilities :

- A denial of service vulnerability exists due to an assertion flaw that is triggered when parsing malformed DNSSEC keys. An unauthenticated, remote attacker can exploit this, via a specially crafted query to a zone containing such a key, to cause a validating resolver to exit. (CVE-2015-5722)

- A denial of service vulnerability exists in the fromwire_openpgpkey() function in openpgpkey_61.c that is triggered when the length of data is less than 1. An unauthenticated, remote attacker can exploit this, via a specially crafted response to a query, to cause an assertion failure that terminates named. (CVE-2015-5986)

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://kb.isc.org/article/AA-01287

https://kb.isc.org/article/AA-01291

Solution

Upgrade to BIND version 9.9.7-P3 / 9.10.2-P4 or later.

Risk Factor

High

VPR Score

3.7

EPSS Score

0.9641

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)

References

CVE	CVE-2015-5722
CVE	CVE-2015-5986

Plugin Information

Published: 2015/09/11, Modified: 2018/06/27

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.7-P3
```

181670 - ISC BIND 9.2.0 < 9.16.44 / 9.9.3-S1 < 9.16.44-S1 / 9.18.0 < 9.18.19 / 9.18.0-S1 < 9.18.19-S1 / 9.19.0 < 9.19.17 Vulnerability (cve-2023-3341)

Synopsis

The remote name server is affected by a vulnerability vulnerability.

Description

The version of ISC BIND installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the cve-2023-3341 advisory.

- The code that processes control channel messages sent to named calls certain functions recursively during packet parsing. Recursion depth is only limited by the maximum accepted packet size; depending on the environment, this may cause the packet-parsing code to run out of available stack memory, causing named to terminate unexpectedly. Since each incoming control channel message is fully parsed before its contents are authenticated, exploiting this flaw does not require the attacker to hold a valid RNDC key;

only network access to the control channel's configured TCP port is necessary.By sending a specially crafted message over the control channel, an attacker can cause the packet-parsing code to run out of available stack memory, causing named to terminate unexpectedly. However, the attack only works in environments where the stack size available to each process/thread is small enough; the exact threshold depends on multiple factors and is therefore impossible to specify universally. (CVE-2023-3341)

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://kb.isc.org/v1/docs/cve-2023-3341

Solution

Upgrade to ISC BIND version 9.16.44 / 9.16.44-S1 / 9.18.19 / 9.18.19-S1 / 9.19.17 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

EPSS Score

0.0005

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-2023-3341
XREF	IAVA:2023-A-0500-S

Plugin Information

Published: 2023/09/20, Modified: 2024/02/16

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.16.44
```

88385 - ISC BIND 9.3.0 < 9.9.8-P3 / 9.9.x-Sx < 9.9.8-S4 / 9.10.x < 9.10.3-P3 Multiple DoS

Synopsis

The remote name server is affected by multiple denial of service vulnerabilities.

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is affected by multiple denial of service vulnerabilities :

- A denial of service vulnerability exists due to improper handling of certain string formatting options. An authenticated, remote attacker can exploit this, via a malformed Address Prefix List (APL) record, to cause an INSIST assertion failure and daemon exit.

(CVE-2015-8704)

- A denial of service vulnerability exists due to a failure to properly convert OPT records and ECS options to formatted text. A remote attacker can exploit this to cause a REQUIRE assertion failure and daemon exit.

Note that this issue only affects BIND 9.10.x.

(CVE-2015-8705)

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://kb.isc.org/article/AA-01335

https://kb.isc.org/article/AA-01336

Solution

Upgrade to BIND version 9.9.8-P3 / 9.9.8-S4 / 9.10.3-P3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.7

EPSS Score

0.9608

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-8704
CVE	CVE-2015-8705

Plugin Information

Published: 2016/01/26, Modified: 2019/11/19

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.8-P3
```

85241 - ISC BIND 9.7.x < 9.9.7-P2 / 9.10.x < 9.10.2-P3 TKEY Query Handling Remote DoS

Synopsis

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

Description

According to its self-reported version number, the installation of ISC BIND on the remote name server is potentially affected by a denial of service vulnerability due to a REQUIRE assertion flaw that occurs while handling TKEY queries. A remote attacker can exploit this by using a specially crafted TKEY query to crash the daemon.

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://kb.isc.org/article/AA-01272

https://kb.isc.org/article/AA-01279

https://kb.isc.org/article/AA-01280

Solution

Upgrade to BIND version 9.9.7-P2 / 9.10.2-P3 or later, or apply the patch referenced in the advisory.

Risk Factor

High

VPR Score

8.1

EPSS Score

0.9669

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

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

References

CVE	CVE-2015-5477
XREF	EDB-ID:37721

Exploitable With

Core Impact (true)

Plugin Information

Published: 2015/08/05, Modified: 2018/06/27

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.7-P2
```

190463 - ISC BIND 9.9.3-S1 < 9.16.48-S1 / 9.0.0 < 9.16.48 / 9.16.8-S1 < 9.16.48-S1 / 9.18.0 < 9.18.24 / 9.18.11-S1 < 9.18.24-S1 / 9.19.0 < 9.19.21 Vulnerability (cve-2023-4408)

Synopsis

The remote name server is affected by a vulnerability vulnerability.

Description

The version of ISC BIND installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the cve-2023-4408 advisory.

- The DNS message parsing code in `named` includes a section whose computational complexity is overly high.

It does not cause problems for typical DNS traffic, but crafted queries and responses may cause excessive CPU load on the affected `named` instance by exploiting this flaw. This issue affects both authoritative servers and recursive resolvers. This issue affects BIND 9 versions 9.0.0 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1. (CVE-2023-4408)

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://kb.isc.org/v1/docs/cve-2023-4408

Solution

Upgrade to ISC BIND version 9.16.48 / 9.16.48-S1 / 9.18.24 / 9.18.24-S1 / 9.19.21 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

EPSS Score

0.0004

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-2023-4408
XREF	IAVA:2024-A-0103-S

Plugin Information

Published: 2024/02/13, Modified: 2024/07/26

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.16.48
```

87502 - ISC BIND 9.x < 9.9.8-P2 / 9.10.x < 9.10.3-P2 Response Parsing Class Attribute Handling DoS

Synopsis

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

Description

According to its self-reported version number, the remote installation of BIND is affected by a denial of service vulnerability due to improper parsing of incorrect class attributes in db.c. An unauthenticated, remote attacker can exploit this, via a malformed class attribute, to trigger a REQUIRE assertion failure, resulting in a denial of service condition.

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://kb.isc.org/docs/aa-01317

http://www.nessus.org/u?06404c1c

Solution

Upgrade to BIND version 9.9.8-P2 / 9.9.8-S3 / 9.10.3-P2 or later.

Note that 9.9.8-S3 is a preview version of BIND provided exclusively to ISC Support customers.

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

EPSS Score

0.9518

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	79349
CVE	CVE-2015-8000

Plugin Information

Published: 2015/12/18, Modified: 2020/04/27

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.8-P2 / 9.9.8-S3 / 9.10.3-P2
```

94611 - ISC BIND 9.x < 9.9.9-P3 Options Sections DoS

Synopsis

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

Description

According to its self-reported version number, the instance of ISC BIND running on the remote name server is 9.x prior to 9.9.9-P3. It is, therefore, affected by a denial of service vulnerability when handling malformed options sections. An unauthenticated, remote attacker can exploit this, via a specially crafted OPT resource record, to cause an assertion failure, resulting in a daemon exit.

See Also

https://kb.isc.org/article/AA-01433

Solution

Upgrade to ISC BIND version 9.9.9-P3 / 9.10.4-P3 / 9.11.0 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

EPSS Score

0.1441

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	93814
CVE	CVE-2016-2848

Plugin Information

Published: 2016/11/08, Modified: 2018/12/07

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.9-P3 / 9.10.4-P3 / 9.11.0
```

100996 - ISC BIND 9.x.x < 9.9.10-P1 / 9.10.x < 9.10.5-P1 / 9.11.x < 9.11.1-P1 Multiple Vulnerabilities

Synopsis

The remote name server is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the instance of ISC BIND running on the remote name server is 9.x.x prior to 9.9.10-P1, 9.10.x prior to 9.10.5-P1, or 9.11.x prior to 9.11.1-P1. It is, therefore, affected by multiple vulnerabilities :

- A denial of service vulnerability exists when processing Response Policy Zone (RPZ) rule types. An unauthenticated, remote attacker can exploit this, via a specially crafted query, to cause an infinite loop condition that degrades the server's functionality.

(CVE-2017-3140)

- A privilege escalation vulnerability exists in the BIND installer for Windows due to using an unquoted service path. A local attacker can exploit this to gain elevated privileges provided that the host file system permissions allow this. Note that non-Windows builds and installations are not affected. (CVE-2017-3141)

See Also

https://kb.isc.org/docs/aa-01495

https://kb.isc.org/docs/aa-01496

Solution

Upgrade to ISC BIND version 9.9.10-P1 / 9.9.10-S2 / 9.10.5-P1 / 9.10.5-S2 / 9.11.1-P1 or later. Note that BIND 9 versions 9.9.10-S2 and 9.10.5-S2 are available exclusively for eligible ISC Support customers.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.1177

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	99088
BID	99089
CVE	CVE-2017-3140
CVE	CVE-2017-3141
XREF	EDB-ID:42121

Plugin Information

Published: 2017/06/22, Modified: 2019/11/13

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.10-P1
```

62119 - ISC BIND Assertion Error Resource Record RDATA Query Parsing Remote DoS

Synopsis

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

Description

According to its self-reported version number, the remote installation of BIND will exit with an assertion failure if a resource record with RDATA in excess of 65535 bytes is loaded and then subsequently queried. Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

See Also

https://kb.isc.org/article/AA-00778/74

http://ftp.isc.org/isc/bind9/9.6-ESV-R7-P3/CHANGES

http://ftp.isc.org/isc/bind9/9.7.6-P3/CHANGES

http://ftp.isc.org/isc/bind9/9.8.3-P3/CHANGES

http://ftp.isc.org/isc/bind9/9.9.1-P3/CHANGES

Solution

Upgrade to BIND 9.6-ESV-R7-P3 / 9.6-ESV-R8 / 9.7.6-P3 / 9.7.7 / 9.8.3-P3 / 9.8.4 / 9.9.1-P3 / 9.9.2 or later.

Risk Factor

High

VPR Score

5.9

EPSS Score

0.3322

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)

References

BID	55522
CVE	CVE-2012-4244

Plugin Information

Published: 2012/09/17, Modified: 2018/09/17

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.6-ESV-R7-P3
```

149211 - ISC BIND DNAME Recursion DoS (CVE-2021-25215)

Synopsis

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

Description

According to its self-reported version, the ISC Bind present on the remote host is affected by a denial of service vulnerability:

- DNAME records, described in RFC 6672, provide a way to redirect a subtree of the domain name tree in the DNS. A flaw in the way named processes these records may trigger an attempt to add the same RRset to the ANSWER section more than once. When a vulnerable version of named receives a query for a record triggering the flaw, the named process will terminate due to a failed assertion check.

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://kb.isc.org/v1/docs/CVE-2021-25215

Solution

Upgrade to the patched release most closely related to your current version of BIND.

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

EPSS Score

0.0208

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-2021-25215
XREF	IAVA:2021-A-0206-S

Plugin Information

Published: 2021/04/30, Modified: 2021/11/09

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.31
```

136769 - ISC BIND Service Downgrade / Reflected DoS

Synopsis

The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities.

Description

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

See Also

https://kb.isc.org/docs/cve-2020-8616

Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.0053

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

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

STIG Severity

I

References

CVE	CVE-2020-8616
XREF	IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/22, Modified: 2024/03/12

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.19
```

17804 - MySQL < 5.0.83 Denial of Service

Synopsis

The remote database server is prone to a denial of service attack.

Description

The version of MySQL installed on the remote host is earlier than 5.0.83 and thus reportedly allows a remote user to crash the server and possibly have other impacts.

See Also

https://seclists.org/fulldisclosure/2009/Jul/58

Solution

Upgrade to MySQL version 5.0.83 or later.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.1739

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	35609
CVE	CVE-2009-2446
XREF	CWE:134

Plugin Information

Published: 2012/01/16, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.0.83
```

17835 - MySQL < 5.0.90 / 5.1.43 / 5.5.0-m2 Multiple Buffer Overflows

Synopsis

The remote database server is affected by several buffer overflow vulnerabilities.

Description

The version of MySQL installed on the remote host is older than 5.0.90, 5.1.43 or 5.5.0-m2. Such versions use yaSSL prior to 1.9.9, that is vulnerable to multiple buffer overflows. These overflows allow a remote attacker to crash the server.

See Also

http://www.nessus.org/u?409fbf00

http://www.nessus.org/u?d46c3ad9

https://bugs.mysql.com/bug.php?id=50227

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-43.html

http://dev.mysql.com/doc/refman/5.0/en/news-5-0-90.html

http://www.nessus.org/u?d50b4e7b

https://lists.mysql.com/commits/96697

https://isc.sans.edu//diary.html?storyid=7900

Solution

Upgrade to MySQL version 5.0.90 / 5.1.43 / 5.5.0-m2 or later.

Risk Factor

High

VPR Score

7.4

EPSS Score

0.9577

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)

References

BID	37640
BID	37943
BID	37974
CVE	CVE-2009-4484
XREF	CWE:119

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2012/01/18, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.0.90
```

34159 - MySQL Community Server 5.0 < 5.0.67 Multiple Vulnerabilities

Synopsis

The remote database server is affected by several issues.

Description

The version of MySQL Community Server 5.0 installed on the remote host is before 5.0.66. Such versions are reportedly affected by the following issues :

- When using a FEDERATED table, a local server could be forced to crash if the remote server returns a result with fewer columns than expected (Bug #29801).

- ALTER VIEW retains the original DEFINER value, even when altered by another user, which could allow that user to gain the access rights of the view (Bug #29908).

- A local user can circumvent privileges through creation of MyISAM tables using the 'DATA DIRECTORY' and 'INDEX DIRECTORY' options to overwrite existing table files in the application's data directory (Bug #32167).

- RENAME TABLE against a table with DATA/INDEX DIRECTORY overwrites the file to which the symlink points (Bug #32111).

- It was possible to force an error message of excessive length, which could lead to a buffer overflow (Bug #32707).

- Three vulnerabilities in yaSSL versions 1.7.5 and earlier as used in MySQL could allow an unauthenticated remote attacker to crash the server or to execute arbitrary code provided yaSSL is enabled and the server allows TCP connections (Bug #33814).

- An empty bit-string literal (b'') used in a SQL statement could result in a server crash (Bug #35658).

See Also

http://dev.mysql.com/doc/refman/5.0/en/news-5-0-67.html

https://lists.mysql.com/announce/542

Solution

Upgrade to MySQL Community Server version 5.0.67.

Risk Factor

High

VPR Score

7.3

EPSS Score

0.9741

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)

References

BID	26765
BID	27140
BID	29106
CVE	CVE-2007-5969
CVE	CVE-2008-0226
CVE	CVE-2008-0227
CVE	CVE-2008-2079
CVE	CVE-2008-3963
CVE	CVE-2008-4098
XREF	CWE:59
XREF	CWE:119
XREF	CWE:134
XREF	CWE:264

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2008/09/11, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
The remote MySQL Community Server's version is :

  5.0.51a-3ubuntu5
```

42256 - NFS Shares World Readable

Synopsis

The remote NFS server exports world-readable shares.

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Solution

Place the appropriate restrictions on all NFS shares.

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 v2.0 Base Score

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

Plugin Information

Published: 2009/10/26, Modified: 2024/02/21

Plugin Output

tcp/2049/rpc-nfs

```
The following shares have no access restrictions :

  / *
```

44081 - OpenSSH < 5.7 Multiple Vulnerabilities

Synopsis

The remote SSH service may be affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is earlier than 5.7. Versions before 5.7 may be affected by the following vulnerabilities :

- A security bypass vulnerability because OpenSSH does not properly validate the public parameters in the J-PAKE protocol. This could allow an attacker to authenticate without the shared secret. Note that this issue is only exploitable when OpenSSH is built with J-PAKE support, which is currently experimental and disabled by default, and that Nessus has not checked whether J-PAKE support is indeed enabled. (CVE-2010-4478)

- The auth_parse_options function in auth-options.c in sshd provides debug messages containing authorized_keys command options, which allows remote, authenticated users to obtain potentially sensitive information by reading these messages. (CVE-2012-0814)

See Also

http://seb.dbzteam.org/crypto/jpake-session-key-retrieval.pdf

http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/Attic/jpake.c#rev1.5

http://www.nessus.org/u?2ac4f8d9

Solution

Upgrade to OpenSSH 5.7 or later.

Risk Factor

High

VPR Score

6.3

EPSS Score

0.0157

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	45304
BID	51702
CVE	CVE-2010-4478
CVE	CVE-2012-0814

Plugin Information

Published: 2011/10/04, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 5.7
```

73079 - OpenSSH < 6.6 Multiple Vulnerabilities

Synopsis

The SSH server on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 6.6. It is, therefore, affected by the following vulnerabilities :

- A flaw exists due to a failure to initialize certain data structures when makefile.inc is modified to enable the J-PAKE protocol. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in a denial of service condition and potentially the execution of arbitrary code. (CVE-2014-1692)

- An error exists related to the 'AcceptEnv' configuration setting in sshd_config due to improper processing of wildcard characters. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to bypass intended environment restrictions.

(CVE-2014-2532)

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

See Also

http://www.openssh.com/txt/release-6.6

https://lists.gt.net/openssh/dev/57663#57663

Solution

Upgrade to OpenSSH version 6.6 or later.

Risk Factor

High

VPR Score

5.3

EPSS Score

0.0364

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	65230
BID	66355
CVE	CVE-2014-1692
CVE	CVE-2014-2532

Plugin Information

Published: 2014/03/18, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 6.6
```

84638 - OpenSSH < 6.9 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 6.9. It is, therefore, affected by the following vulnerabilities :

- A flaw exists within the x11_open_helper() function in the 'channels.c' file that allows connections to be permitted after 'ForwardX11Timeout' has expired. A remote attacker can exploit this to bypass timeout checks and XSECURITY restrictions. (CVE-2015-5352)

- Various issues were addressed by fixing the weakness in agent locking by increasing the failure delay, storing the salted hash of the password, and using a timing-safe comparison function.

- An out-of-bounds read error exists when handling incorrect pattern lengths. A remote attacker can exploit this to cause a denial of service or disclose sensitive information in the memory.

- An out-of-bounds read error exists when parsing the 'EscapeChar' configuration option.

See Also

http://www.openssh.com/txt/release-6.9

http://www.nessus.org/u?725c4682

Solution

Upgrade to OpenSSH 6.9 or later.

Risk Factor

High

VPR Score

3.4

EPSS Score

0.0092

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	75525
CVE	CVE-2015-5352

Plugin Information

Published: 2015/07/09, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 6.9
```

93194 - OpenSSH < 7.3 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.3. It is, therefore, affected by multiple vulnerabilities :

- A local privilege escalation when the UseLogin feature is enabled and PAM is configured to read .pam_environment files from home directories. (CVE-2015-8325)

- A flaw exists that is due to the program returning shorter response times for authentication requests with overly long passwords for invalid users than for valid users. This may allow a remote attacker to conduct a timing attack and enumerate valid usernames.

(CVE-2016-6210)

- A denial of service vulnerability exists in the auth_password() function in auth-passwd.c due to a failure to limit password lengths for password authentication. An unauthenticated, remote attacker can exploit this, via a long string, to consume excessive CPU resources, resulting in a denial of service condition. (CVE-2016-6515)

- An unspecified flaw exists in the CBC padding oracle countermeasures that allows an unauthenticated, remote attacker to conduct a timing attack.

- A flaw exists due to improper operation ordering of MAC verification for Encrypt-then-MAC (EtM) mode transport MAC algorithms when verifying the MAC before decrypting any ciphertext. An unauthenticated, remote attacker can exploit this, via a timing attack, to disclose sensitive information.

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

See Also

http://www.openssh.com/txt/release-7.3

https://marc.info/?l=openbsd-announce&m=147005433429403

Solution

Upgrade to OpenSSH version 7.3 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0688

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	86187
BID	92212
CVE	CVE-2015-8325
CVE	CVE-2016-6515
CVE	CVE-2016-6210

Plugin Information

Published: 2016/08/29, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 7.3
```

96151 - OpenSSH < 7.4 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.4. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists in ssh-agent due to loading PKCS#11 modules from paths that are outside a trusted whitelist.

A local attacker can exploit this, by using a crafted request to load hostile modules via agent forwarding, to execute arbitrary code. To exploit this vulnerability, the attacker would need to control the forwarded agent-socket (on the host running the sshd server) and the ability to write to the file system of the host running ssh-agent. (CVE-2016-10009)

- A flaw exists in sshd due to creating forwarded Unix-domain sockets with 'root' privileges whenever privilege separation is disabled. A local attacker can exploit this to gain elevated privileges.

(CVE-2016-10010)

- An information disclosure vulnerability exists in sshd within the realloc() function due leakage of key material to privilege-separated child processes when reading keys. A local attacker can possibly exploit this to disclose sensitive key material. Note that no such leak has been observed in practice for normal-sized keys, nor does a leak to the child processes directly expose key material to unprivileged users.

(CVE-2016-10011)

- A flaw exists in sshd within the shared memory manager used by pre-authenticating compression support due to a bounds check being elided by some optimizing compilers and due to the memory manager being incorrectly accessible when pre-authenticating compression is disabled. A local attacker can exploit this to gain elevated privileges. (CVE-2016-10012)

- A denial of service vulnerability exists in sshd when handling KEXINIT messages. An unauthenticated, remote attacker can exploit this, by sending multiple KEXINIT messages, to consume up to 128MB per connection.

- A flaw exists in sshd due to improper validation of address ranges by the AllowUser and DenyUsers directives at configuration load time. A local attacker can exploit this, via an invalid CIDR address range, to gain access to restricted areas.

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

See Also

http://www.openssh.com/txt/release-7.4

Solution

Upgrade to OpenSSH version 7.4 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

EPSS Score

0.1089

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	94968
BID	94972
BID	94975
BID	94977
CVE	CVE-2016-10009
CVE	CVE-2016-10010
CVE	CVE-2016-10011
CVE	CVE-2016-10012
CVE	CVE-2016-10708
XREF	EDB-ID:40962

Plugin Information

Published: 2016/12/27, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 7.4
```

35043 - PHP 5 < 5.2.7 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 prior to 5.2.7. It is, therefore, affected by multiple vulnerabilities :

- There is a buffer overflow flaw in the bundled PCRE library that allows a denial of service attack.

(CVE-2008-2371)

- Multiple directory traversal vulnerabilities exist in functions such as 'posix_access', 'chdir', and 'ftok'

that allow a remote attacker to bypass 'safe_mode'

restrictions. (CVE-2008-2665 and CVE-2008-2666).

- A buffer overflow flaw in 'php_imap.c' may be triggered when processing long message headers due to the use of obsolete API calls. This can be exploited to cause a denial of service or to execute arbitrary code.

(CVE-2008-2829)

- A buffer overflow in the 'imageloadfont' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. This can be exploited to cause a denial of service or to execute arbitrary code. (CVE-2008-3658)

- A buffer overflow flaw exists in PHP's internal function 'memnstr' which can be exploited by an attacker using the delimiter argument to the 'explode' function. This can be used to cause a denial of service or to execute arbitrary code. (CVE-2008-3659)

- When PHP is used as a FastCGI module, an attacker by requesting a file whose file name extension is preceded by multiple dots can cause a denial of service.

(CVE-2008-3660)

- A heap-based buffer overflow flaw in the mbstring extension can be triggered via a specially crafted string containing an HTML entity that is not handled during Unicode conversion. This can be exploited to execute arbitrary code.(CVE-2008-5557)

- Improper initialization of global variables 'page_uid'

and 'page_gid' when PHP is used as an Apache module allows the bypassing of security restriction due to SAPI 'php_getuid' function overloading. (CVE-2008-5624)

- PHP does not enforce the correct restrictions when 'safe_mode' is enabled through a 'php_admin_flag'

setting in 'httpd.conf'. This allows an attacker, by placing a specially crafted 'php_value' entry in '.htaccess', to able to write to arbitrary files.

(CVE-2008-5625)

- The 'ZipArchive::extractTo' function in the ZipArchive extension fails to filter directory traversal sequences from file names. An attacker can exploit this to write to arbitrary files. (CVE-2008-5658)

- Under limited circumstances, an attacker can cause a file truncation to occur when calling the 'dba_replace'

function with an invalid argument. (CVE-2008-7068)

- A buffer overflow error exists in the function 'date_from_ISO8601' function within file 'xmlrpc.c' because user-supplied input is improperly validated.
This can be exploited by a remote attacker to cause a denial of service or to execute arbitrary code. (CVE-2014-8626)

See Also

http://cxsecurity.com/issue/WLB-2008110041
http://cxsecurity.com/issue/WLB-2008110058
http://cxsecurity.com/issue/WLB-2008120011
https://seclists.org/fulldisclosure/2008/Jun/237
https://seclists.org/fulldisclosure/2008/Jun/238
https://www.openwall.com/lists/oss-security/2008/08/08/2
https://www.openwall.com/lists/oss-security/2008/08/13/8
https://seclists.org/fulldisclosure/2008/Nov/674
https://seclists.org/fulldisclosure/2008/Dec/90
https://bugs.php.net/bug.php?id=42862
https://bugs.php.net/bug.php?id=45151
https://bugs.php.net/bug.php?id=45722
http://www.php.net/releases/5_2_7.php
http://www.php.net/ChangeLog-5.php#5.2.7

Solution

Upgrade to PHP version 5.2.8 or later.

Note that version 5.2.7 has been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc'
setting remaining off even if it was set to on.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.162

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	29796
BID	29797
BID	29829
BID	30087
BID	30649
BID	31612
BID	32383
BID	32625
BID	32688
BID	32948
BID	70928
CVE	CVE-2008-2371
CVE	CVE-2008-2665
CVE	CVE-2008-2666
CVE	CVE-2008-2829
CVE	CVE-2008-3658
CVE	CVE-2008-3659
CVE	CVE-2008-3660
CVE	CVE-2008-5557
CVE	CVE-2008-5624
CVE	CVE-2008-5625
CVE	CVE-2008-5658
CVE	CVE-2008-7068
CVE	CVE-2014-8626
XREF	CWE:20
XREF	CWE:22
XREF	CWE:119
XREF	CWE:264

Plugin Information

Published: 2008/12/05, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.7
```

48244 - PHP 5.2 < 5.2.14 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP 5.2 installed on the remote host is older than 5.2.14. Such versions may be affected by several security issues :

- An error exists when processing invalid XML-RPC requests that can lead to a NULL pointer dereference. (bug #51288) (CVE-2010-0397)

- An error exists in the function 'fnmatch' that can lead to stack exhaustion.

- An error exists in the sqlite extension that could allow arbitrary memory access.

- A memory corruption error exists in the function 'substr_replace'.

- The following functions are not properly protected against function interruptions :

addcslashes, chunk_split, html_entity_decode, iconv_mime_decode, iconv_substr, iconv_mime_encode, htmlentities, htmlspecialchars, str_getcsv, http_build_query, strpbrk, strstr, str_pad, str_word_count, wordwrap, strtok, setcookie, strip_tags, trim, ltrim, rtrim, parse_str, pack, unpack, uasort, preg_match, strrchr, strchr, substr, str_repeat (CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2484)

- The following opcodes are not properly protected against function interruptions :

ZEND_CONCAT, ZEND_ASSIGN_CONCAT, ZEND_FETCH_RW (CVE-2010-2191)

- The default session serializer contains an error that can be exploited when assigning session variables having user defined names. Arbitrary serialized values can be injected into sessions by including the PS_UNDEF_MARKER, '!', character in variable names.

- A use-after-free error exists in the function 'spl_object_storage_attach'. (CVE-2010-2225)

- An information disclosure vulnerability exists in the function 'var_export' when handling certain error conditions. (CVE-2010-2531)

See Also

http://www.php.net/releases/5_2_14.php

http://www.php.net/ChangeLog-5.php#5.2.14

Solution

Upgrade to PHP version 5.2.14 or later.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.0368

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	38708
BID	40948
BID	41991
CVE	CVE-2007-1581
CVE	CVE-2010-0397
CVE	CVE-2010-1860
CVE	CVE-2010-1862
CVE	CVE-2010-1864
CVE	CVE-2010-2097
CVE	CVE-2010-2100
CVE	CVE-2010-2101
CVE	CVE-2010-2190
CVE	CVE-2010-2191
CVE	CVE-2010-2225
CVE	CVE-2010-2484
CVE	CVE-2010-2531
CVE	CVE-2010-3065
XREF	SECUNIA:39675
XREF	SECUNIA:40268

Plugin Information

Published: 2010/08/04, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.14
```

41014 - PHP < 5.2.11 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues :

- An unspecified error occurs in certificate validation inside 'php_openssl_apply_verification_policy'.

- An unspecified input validation vulnerability affects the color index in 'imagecolortransparent()'.

- An unspecified input validation vulnerability affects exif processing.

- Calling 'popen()' with an invalid mode can cause a crash under Windows. (Bug #44683)

- An integer overflow in 'xml_utf8_decode()' can make it easier to bypass cross-site scripting and SQL injection protection mechanisms using a specially crafted string with a long UTF-8 encoding. (Bug #49687)

- 'proc_open()' can bypass 'safe_mode_protected_env_vars'.
(Bug #49026)

See Also

http://www.php.net/ChangeLog-5.php#5.2.11

http://www.php.net/releases/5_2_11.php

http://news.php.net/php.internals/45597

http://www.php.net/ChangeLog-5.php#5.2.11

Solution

Upgrade to PHP version 5.2.11 or later.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.0218

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	36449
BID	44889
CVE	CVE-2009-3291
CVE	CVE-2009-3292
CVE	CVE-2009-3293
CVE	CVE-2009-3294
CVE	CVE-2009-4018
CVE	CVE-2009-5016
XREF	SECUNIA:36791
XREF	CWE:20
XREF	CWE:134
XREF	CWE:264

Plugin Information

Published: 2009/09/18, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.11
```

32123 - PHP < 5.2.6 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.6. Such versions may be affected by the following issues :

- A stack-based buffer overflow in FastCGI SAPI.

- An integer overflow in printf().

- An security issue arising from improper calculation of the length of PATH_TRANSLATED in cgi_main.c.

- A safe_mode bypass in cURL.

- Incomplete handling of multibyte chars inside escapeshellcmd().

- Issues in the bundled PCRE fixed by version 7.6.

See Also

https://seclists.org/bugtraq/2008/Mar/285

https://seclists.org/fulldisclosure/2008/May/102

https://seclists.org/fulldisclosure/2008/May/106

http://www.php.net/releases/5_2_6.php

Solution

Upgrade to PHP version 5.2.6 or later.

Risk Factor

High

VPR Score

7.4

EPSS Score

0.7069

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	27413
BID	28392
BID	29009
CVE	CVE-2007-4850
CVE	CVE-2007-6039
CVE	CVE-2008-0599
CVE	CVE-2008-1384
CVE	CVE-2008-2050
CVE	CVE-2008-2051
XREF	SECUNIA:30048
XREF	CWE:20
XREF	CWE:119
XREF	CWE:264

Plugin Information

Published: 2008/05/02, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.6
```

35067 - PHP < 5.2.8 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that may be affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.2.8. As such, it is potentially affected by the following vulnerabilities :

- PHP fails to properly sanitize error messages of arbitrary HTML or script code, would code allow for cross-site scripting attacks if PHP's 'display_errors' setting is enabled. (CVE-2008-5814)

- Version 5.2.7 introduced a regression with regard to 'magic_quotes' functionality due to an incorrect fix to the filter extension. As a result, the 'magic_quotes_gpc' setting remains off even if it is set to on. (CVE-2008-5844)

See Also

https://bugs.php.net/bug.php?id=42718

http://www.php.net/releases/5_2_8.php

Solution

Upgrade to PHP version 5.2.8 or later.

Risk Factor

High

VPR Score

6.3

EPSS Score

0.0032

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	32673
CVE	CVE-2008-5814
CVE	CVE-2008-5844
XREF	CWE:16
XREF	CWE:79

Plugin Information

Published: 2008/12/09, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.8
```

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

9.0

EPSS Score

0.9569

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: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.3.12 / 5.4.2
```

57537 - PHP < 5.3.9 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.9. As such, it may be affected by the following security issues :

- The 'is_a()' function in PHP 5.3.7 and 5.3.8 triggers a call to '__autoload()'. (CVE-2011-3379)

- It is possible to create a denial of service condition by sending multiple, specially crafted requests containing parameter values that cause hash collisions when computing the hash values for storage in a hash table. (CVE-2011-4885)

- An integer overflow exists in the exif_process_IFD_TAG function in exif.c that can allow a remote attacker to read arbitrary memory locations or cause a denial of service condition. This vulnerability only affects PHP 5.4.0beta2 on 32-bit platforms. (CVE-2011-4566)

- Calls to libxslt are not restricted via xsltSetSecurityPrefs(), which could allow an attacker to create or overwrite files, resulting in arbitrary code execution. (CVE-2012-0057)

- An error exists in the function 'tidy_diagnose' that can allow an attacker to cause the application to dereference a NULL pointer. This causes the application to crash. (CVE-2012-0781)

- The 'PDORow' implementation contains an error that can cause application crashes when interacting with the session feature. (CVE-2012-0788)

- An error exists in the timezone handling such that repeated calls to the function 'strtotime' can allow a denial of service attack via memory consumption.

(CVE-2012-0789)

See Also

https://www.tenable.com/security/research/tra-2012-01

http://xhe.myxwiki.org/xwiki/bin/view/XSLT/Application_PHP5

http://www.php.net/archive/2012.php#id2012-01-11-1

https://seclists.org/bugtraq/2012/Jan/91

https://bugs.php.net/bug.php?id=55475

https://bugs.php.net/bug.php?id=55776

https://bugs.php.net/bug.php?id=53502

http://www.php.net/ChangeLog-5.php#5.3.9

Solution

Upgrade to PHP version 5.3.9 or later.

Risk Factor

High

VPR Score

6.3

EPSS Score

0.8473

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	49754
BID	50907
BID	51193
BID	51806
BID	51952
BID	51992
BID	52043
CVE	CVE-2011-3379
CVE	CVE-2011-4566
CVE	CVE-2011-4885
CVE	CVE-2012-0057
CVE	CVE-2012-0781
CVE	CVE-2012-0788
CVE	CVE-2012-0789
XREF	TRA:TRA-2012-01

Exploitable With

Core Impact (true)

Plugin Information

Published: 2012/01/13, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.3.9
```

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: 2024/11/22

Plugin Output

tcp/80/www

```
  URL               : http://Epic-Metasploitable.epicode/ (5.2.4-2ubuntu5.10 under X-Powered-By:
PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/phpinfo.php)
  Installed version : 5.2.4-2ubuntu5.10
  Fixed version     : 7.3.24
```

59088 - PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution

Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution.

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

See Also

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

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

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

http://www.php.net/ChangeLog-5.php#5.4.3

http://www.nessus.org/u?80589ce8

https://www-304.ibm.com/support/docview.wss?uid=swg21620314

Solution

If using Lotus Foundations, upgrade the Lotus Foundations operating system to version 1.2.2b or later.

Otherwise, upgrade to PHP 5.3.13 / 5.4.3 or later.

Risk Factor

High

VPR Score

9.0

EPSS Score

0.9569

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
CVE	CVE-2012-2311
XREF	CERT:520827
XREF	EDB-ID:18834
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

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

Plugin Information

Published: 2012/05/14, Modified: 2022/03/28

Plugin Output

tcp/80/www

```
Nessus was able to verify the issue exists using the following request :

------------------------------ snip ------------------------------
POST /dvwa/dvwa/includes/DBMS/DBMS.php?-d+allow_url_include%3don+-d+safe_mode%3doff+-d
+suhosin.simulation%3don+-d+open_basedir%3doff+-d+auto_prepend_file%3dphp%3a//input+-n HTTP/1.1
Host: Epic-Metasploitable.epicode
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 82
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, */*
<?php echo 'php_cgi_query_string_code_execution-1739154185'; system('id'); die; ?>
------------------------------ snip ------------------------------

This produced the following output :

------------------------------ snip ------------------------------
uid=33(www-data) gid=33(www-data) groups=33(www-data)
------------------------------ snip ------------------------------
```

63349 - PostgreSQL 7.4 < 7.4.29 / 8.0 < 8.0.25 / 8.1 < 8.1.21 / 8.2 < 8.2.17 / 8.3 < 8.3.11 / 8.4 < 8.4.4 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of PostgreSQL installed on the remote host is 7.4 prior to 7.4.29, 8.0 prior to 8.0.25, 8.1 prior to 8.1.21, 8.2 prior to 8.2.17, 8.3 prior to 8.3.11 or 8.4 prior to 8.4.4. As such, it is potentially affected by multiple vulnerabilities :

- A vulnerability in Safe.pm and PL/Perl can allow an authenticated user to run arbitrary Perl code on the database server if PL/Perl is installed and enabled.

(CVE-2010-1169)

- Insecure permissions on the pltcl_modules table could allow an authenticated user to run arbitrary Tcl code on the database server if PL/Tcl is installed and enabled. (CVE-2010-1170)

- An unprivileged database user can remove superuser-only settings that were applied to the user's account with ALTER USER by a superuser thus bypassing settings that should be enforced. (CVE-2010-1975)

See Also

https://www.postgresql.org/about/news/1203/

https://www.postgresql.org/docs/7.4/release-7-4-29.html

https://www.postgresql.org/docs/8.0/release-8-0-25.html

https://www.postgresql.org/docs/8.1/release-8-1-21.html

https://www.postgresql.org/docs/8.2/release-8-2-17.html

http://www.postgresql.org/docs/8.3/static/release-8-3-11.html

http://www.postgresql.org/docs/8.4/static/release-8-4-4.html

Solution

Upgrade to PostgreSQL 7.4.29 / 8.0.25 / 8.1.21 / 8.2.17 / 8.3.11 / 8.4.4 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0058

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	40215
BID	40304
CVE	CVE-2010-1169
CVE	CVE-2010-1170
CVE	CVE-2010-1975

Plugin Information

Published: 2012/12/28, Modified: 2024/10/23

Plugin Output

tcp/5432/postgresql

```
Version source    : Fauth.c.L1003.Rauth_failed
Installed version : 8.3.8
Fixed version     : 7.4.29 / 8.0.25 / 8.1.21 / 8.2.17 / 8.3.11 / 8.4.4
```

63355 - PostgreSQL 8.3 < 8.3.18 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of PostgreSQL installed on the remote host is 8.3.x prior to 8.3.18, and is, therefore, potentially affected by multiple vulnerabilities :

- Permissions on a function called by a trigger are not properly checked. (CVE-2012-0866)

- Line breaks in object names can be exploited to execute arbitrary SQL commands when reloading a pg_dump file.

(CVE-2012-0868)

See Also

http://www.postgresql.org/about/news/1377/

https://www.postgresql.org/docs/8.3/release-8-3-18.html

Solution

Upgrade to PostgreSQL 8.3.18 or later.

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

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

VPR Score

5.9

EPSS Score

0.0099

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	52188
CVE	CVE-2012-0866
CVE	CVE-2012-0868

Plugin Information

Published: 2012/12/28, Modified: 2024/10/23

Plugin Output

tcp/5432/postgresql

```
Version source    : Fauth.c.L1003.Rauth_failed
Installed version : 8.3.8
Fixed version     : 8.3.18
```

63353 - PostgreSQL 8.3 < 8.3.19 / 8.4 < 8.4.12 / 9.0 < 9.0.8 / 9.1 < 9.1.4 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of PostgreSQL installed on the remote host is 8.3.x prior to 8.3.19, 8.4.x prior to 8.4.12, 9.0.x prior to 9.0.8, or 9.1.x prior to 9.1.4. As such, it is potentially affected by multiple vulnerabilities :

- Passwords containing the byte 0x80 passed to the crypt() function in pgcrypto are incorrectly truncated if DES encryption was used. (CVE-2012-2143)

- SECURITY_DEFINER and SET attributes on procedural call handlers are not ignored and can be used to crash the server. (CVE-2012-2655)

See Also

https://www.postgresql.org/about/news/1398/

https://www.postgresql.org/docs/8.3/release-8-3-19.html

https://www.postgresql.org/docs/8.4/release-8-4-12.html

https://www.postgresql.org/docs/9.0/release-9-0-8.html

https://www.postgresql.org/docs/9.1/release-9-1-4.html

Solution

Upgrade to PostgreSQL 8.3.19 / 8.4.12 / 9.0.8 / 9.1.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.3

EPSS Score

0.0116

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	53729
BID	53812
CVE	CVE-2012-2143
CVE	CVE-2012-2655

Plugin Information

Published: 2012/12/28, Modified: 2024/10/23

Plugin Output

tcp/5432/postgresql

```
Version source    : Fauth.c.L1003.Rauth_failed
Installed version : 8.3.8
Fixed version     : 8.3.19 / 8.4.12 / 9.0.8 / 9.1.4
```

106750 - ProFTPD 1.3.1 SQL injection protection bypass

Synopsis

The remote FTP server is affected by a mitigation bypass.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

According to its banner, the version of ProFTPD installed on the remote host is 1.3.1x and may be affected by SQL injection protection bypass when NLS support is enabled.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=3173

Solution

Upgrade to ProFTPD version 1.3.2 or later.

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

4.2

EPSS Score

0.0034

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)

References

BID	33650
CVE	CVE-2009-0543
XREF	CWE:89

Plugin Information

Published: 2018/02/12, Modified: 2019/11/08

Plugin Output

tcp/2121/ftp

```
  Version source    : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
500 GET not understood
  Installed version : 1.3.1
  Fixed version     : 1.3.2
```

56956 - ProFTPD < 1.3.3g / 1.3.4 Response Pool Use-After-Free Code Execution

Synopsis

The remote FTP server is affected by a code execution vulnerability.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

According to its banner, the version of ProFTPD installed on the remote host is earlier than 1.3.3g or 1.3.4. As such, it is potentially affected by a code execution vulnerability due to how the server manages the response pool that is used to send responses from the server to the client. A remote, authenticated attacker could leverage this issue to execute arbitrary code on the remote host, subject to the privileges of the user running the affected application.

Note that Nessus did not actually test for the flaw but instead has relied on the version in ProFTPD's banner.

See Also

https://www.zerodayinitiative.com/advisories/ZDI-11-328/

https://seclists.org/fulldisclosure/2011/Nov/174

http://bugs.proftpd.org/show_bug.cgi?id=3711

http://www.nessus.org/u?c4b46de4

http://www.nessus.org/u?3c33326d

Solution

Upgrade to ProFTPD version 1.3.3g / 1.3.4 or later.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.0176

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	50631
CVE	CVE-2011-4130

Plugin Information

Published: 2011/11/28, Modified: 2020/03/27

Plugin Output

tcp/2121/ftp

```
  Version source    : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
500 GET not understood
  Installed version : 1.3.1
  Fixed version     : 1.3.3g / 1.3.4
```

106755 - ProFTPD < 1.3.5b / 1.3.6x < 1.3.6rc2 weak Diffie-Hellman key

Synopsis

The remote FTP server is affected by a Denial of Service vulnerability.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

According to its banner, the version of ProFTPD installed on the remote host is prior to 1.3.5b or 1.3.6x prior to 1.3.6rc2 and is affected by an issue in the mod_tls module, which might cause a weaker than intended Diffie-Hellman key to be used.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=4230

Solution

Upgrade to ProFTPD version 1.3.5b / 1.3.6rc2 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

EPSS Score

0.005

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	84327
CVE	CVE-2016-3125

Plugin Information

Published: 2018/02/12, Modified: 2019/11/08

Plugin Output

tcp/2121/ftp

```
  Version source    : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
500 GET not understood
  Installed version : 1.3.1
  Fixed version     : 1.3.5b / 1.3.6rc2
```

47036 - Samba 3.x < 3.3.13 SMB1 Packet Chaining Memory Corruption

Synopsis

The remote service is affected by a memory corruption vulnerability.

Description

According to its banner, the version of Samba running on the remote host is a version of 3.x before 3.3.13. Such versions are affected by a memory corruption vulnerability when handling specially crafted SMB1 packets.

By exploiting this flaw, a remote, unauthenticated attacker could crash the affected service or potentially execute arbitrary code subject to the privileges of the user running the affected application.

See Also

https://www.samba.org/samba/security/CVE-2010-2063.html

https://www.samba.org/samba/history/security.html

Solution

Upgrade to Samba 3.3.13 or later.

Risk Factor

High

VPR Score

7.4

EPSS Score

0.9706

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)

References

BID	40884
CVE	CVE-2010-2063

XREF Secunia:40145

Exploitable With

Metasploit (true)

Plugin Information

Published: 2010/06/17, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
The remote Samba server appears to be :

  Samba 3.0.20-Debian
```

49228 - Samba 3.x < 3.5.5 / 3.4.9 / 3.3.14 sid_parse Buffer Overflow

Synopsis

The remote Samba server is affected by a buffer overflow vulnerability.

Description

According to its banner, the version of Samba 3.x running on the remote host is earlier than 3.5.5. The 'sid_parse()' and related 'dom_sid_parse()' functions in such versions fail to correctly check their input lengths when reading a binary representation of a Windows SID (Security ID).

An attacker who is able to get a connection to a file share, either authenticated or via a guest connection, can leverage this issue to launch a stack-based buffer overflow attack against the affected smbd service and possibly execute arbitrary code.

Note that Nessus has not actually tried to exploit this issue or determine if one of the patches has been applied.

See Also

https://bugzilla.samba.org/show_bug.cgi?id=7669

https://www.samba.org/samba/security/CVE-2010-3069.html

https://www.samba.org/samba/history/samba-3.5.5.html

https://www.samba.org/samba/history/samba-3.4.9.html

https://www.samba.org/samba/history/samba-3.3.14.html

Solution

Either apply one of the patches referenced in the project's advisory or upgrade to 3.5.5 / 3.4.9 / 3.3.14 or later.

Risk Factor

High

VPR Score

5.9

EPSS Score

0.8775

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	43212
CVE	CVE-2010-3069
XREF	Secunia:41354

Plugin Information

Published: 2010/09/15, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Installed version  : 3.0.20-Debian
Fixed version      : 3.5.5 / 3.4.9 / 3.3.14
```

90508 - Samba 3.x < 4.2.10 / 4.2.x < 4.2.10 / 4.3.x < 4.3.7 / 4.4.x < 4.4.1 Multiple Vulnerabilities (Badlock)

Synopsis

The remote Samba server is affected by multiple vulnerabilities.

Description

The version of Samba running on the remote host is 3.x or 4.2.x prior to 4.2.10, 4.3.x prior to 4.3.7, or 4.4.x prior to 4.4.1. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists in the DCE-RPC client when handling specially crafted DCE-RPC packets. A man-in-the-middle (MitM) attacker can exploit this to downgrade the connection security, cause a denial of service through resource exhaustion, or potentially execute arbitrary code. (CVE-2015-5370)

- A flaw exists in the implementation of NTLMSSP authentication. A MitM attacker can exploit this to clear the NTLMSSP_NEGOTIATE_SIGN and NTLMSSP_NEGOTIATE_SEAL settings, take over the connections, cause traffic to be sent unencrypted, or have other unspecified impact. (CVE-2016-2110)

- A flaw exists in NETLOGON due to a failure to properly establish a secure channel connection. A MitM attacker can exploit this to spoof the computer names of a secure channel's endpoints, potentially gaining session information. (CVE-2016-2111)

- A flaw exists in the integrity protection mechanisms that allows a MitM attacker to downgrade a secure LDAP connection to an insecure version. (CVE-2016-2112)

- A flaw exists due to improper validation of TLS certificates for the LDAP and HTTP protocols. A MitM attacker can exploit this, via a crafted certificate, to spoof a server, resulting in the disclosure or manipulation of the transmitted traffic. (CVE-2016-2113)

- A flaw exists due to a failure to enforce the 'server signing = mandatory' option in smb.conf for clients using the SMB1 protocol. A MitM attacker can exploit this to conduct spoofing attacks.

(CVE-2016-2114)

- A flaw exists due to a failure to perform integrity checking for SMB client connections. A MitM attacker can exploit this to conduct spoofing attacks since the protection mechanisms for DCERPC communication sessions are inherited from the underlying SMB connection.

(CVE-2016-2115)

- A flaw, known as Badlock, exists 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 MitM attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

(CVE-2016-2118)

See Also

https://www.samba.org/samba/security/CVE-2015-5370.html

https://www.samba.org/samba/security/CVE-2016-2110.html

https://www.samba.org/samba/security/CVE-2016-2111.html
https://www.samba.org/samba/security/CVE-2016-2112.html
https://www.samba.org/samba/security/CVE-2016-2113.html
https://www.samba.org/samba/security/CVE-2016-2114.html
https://www.samba.org/samba/security/CVE-2016-2115.html
https://www.samba.org/samba/security/CVE-2016-2118.html
https://www.samba.org/samba/history/samba-4.2.10.html
https://www.samba.org/samba/history/samba-4.3.7.html
https://www.samba.org/samba/history/samba-4.4.1.html
http://badlock.org

Solution

Upgrade to Samba version 4.2.10 / 4.3.7 / 4.4.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0489

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	86002

CVE	CVE-2015-5370
CVE	CVE-2016-2110
CVE	CVE-2016-2111
CVE	CVE-2016-2112
CVE	CVE-2016-2113
CVE	CVE-2016-2114
CVE	CVE-2016-2115
CVE	CVE-2016-2118
XREF	CERT:813296

Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Installed version : 3.0.20-Debian
Fixed version     : 4.2.10
```

24685 - Samba < 3.0.24 Multiple Flaws

Synopsis

The remote Samba server is affected by several vulnerabilities that could lead to remote code execution

Description

According to its version number, the remote Samba server is affected by several flaws :

- A denial of service issue occuring if an authenticated attacker sends a large number of CIFS session requests which will cause an infinite loop to occur in the smbd daemon, thus utilizing CPU resources and denying access to legitimate users ;

- A remote format string vulnerability that could be exploited by an attacker with write access to a remote share by sending a malformed request to the remote service (this issue only affects installations sharing an AFS file system when the afsacl.so VFS module is loaded)

- A remote buffer overflow vulnerability affecting the NSS lookup capability of the remote winbindd daemon

Solution

Upgrade to Samba 3.0.24 or newer

Risk Factor

High

VPR Score

5.8

EPSS Score

0.0304

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	22395
BID	22403
BID	22410

CVE	CVE-2007-0452
CVE	CVE-2007-0453
CVE	CVE-2007-0454

Plugin Information

Published: 2007/02/22, Modified: 2018/07/27

Plugin Output

tcp/445/cifs

28228 - Samba < 3.0.27 Multiple Vulnerabilities

Synopsis

The remote Samba server may be affected one or more vulnerabilities.

Description

According to its banner, the version of the Samba server on the remote host contains a boundary error in the 'reply_netbios_packet()'

function in 'nmbd/nmbd_packets.c' when sending NetBIOS replies.

Provided the server is configured to run as a WINS server, a remote attacker can exploit this issue by sending multiple specially crafted WINS 'Name Registration' requests followed by a WINS 'Name Query'

request, leading to a stack-based buffer overflow. This could also allow for the execution of arbitrary code.

There is also a stack buffer overflow in nmbd's logon request processing code that can be triggered by means of specially crafted GETDC mailslot requests when the affected server is configured as a Primary or Backup Domain Controller. Note that the Samba security team currently does not believe this particular issue can be exploited to execute arbitrary code remotely.

See Also

https://secuniaresearch.flexerasoftware.com/secunia_research/2007-90/advisory/

https://www.securityfocus.com/archive/1/483744

http://us1.samba.org/samba/security/CVE-2007-4572.html

http://us1.samba.org/samba/security/CVE-2007-5398.html

https://www.securityfocus.com/archive/1/483742

https://www.securityfocus.com/archive/1/483743

Solution

Upgrade to Samba version 3.0.27 or later.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.9617

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

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

References

BID	26454
BID	26455
CVE	CVE-2007-4572
CVE	CVE-2007-5398
XREF	CWE:119

Plugin Information

Published: 2007/11/16, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

29253 - Samba < 3.0.28 send_mailslot Function Remote Buffer Overflow

Synopsis

The remote Samba server may be affected by a buffer overflow vulnerability.

Description

According to its banner, the version of the Samba server on the remote host is reportedly affected by a boundary error in 'nmbd' within the 'send_mailslot' function. Provided the 'domain logons' option is enabled in 'smb.conf', an attacker can leverage this issue to produce a stack-based buffer overflow using a 'SAMLOGON' domain logon packet in which the username string is placed at an odd offset and is followed by a long 'GETDC' string.

Note that Nessus has not actually tried to exploit this issue nor verify whether the 'domain logons' option has been enabled on the remote host.

See Also

https://secuniaresearch.flexerasoftware.com/secunia_research/2007-99/advisory/

https://www.securityfocus.com/archive/1/484818/30/0/threaded

https://www.samba.org/samba/security/CVE-2007-6015.html

Solution

Upgrade to Samba version 3.0.28 or later.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.9718

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)

References

BID	26791
CVE	CVE-2007-6015
XREF	CWE:119

Plugin Information

Published: 2007/12/10, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

32476 - Samba < 3.0.30 receive_smb_raw Function Remote Buffer Overflow

Synopsis

The remote Samba server may be affected by a buffer overflow vulnerability.

Description

According to its banner, the version of the Samba server on the remote host is reportedly affected by a boundary error in 'nmbd' within the 'receive_smb_raw' function in 'lib/util_sock.c' when parsing SMB packets received in a client context. By sending specially crafted packets to an 'nmbd' server configured as a local or domain master browser, an attacker can leverage this issue to produce a heap-based buffer overflow and execute arbitrary code with system privileges.

Note that Nessus has not actually tried to exploit this issue, verify the remote 'nmbd' server's configuration, or determine if the fix has been applied.

See Also

https://secuniaresearch.flexerasoftware.com/secunia_research/2008-20/advisory/

https://www.samba.org/samba/security/CVE-2008-1105.html

https://seclists.org/bugtraq/2008/May/328

Solution

Upgrade to Samba version 3.0.30 or later or apply the patch referenced in the project's advisory.

Risk Factor

High

VPR Score

6.0

EPSS Score

0.9599

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	29404
CVE	CVE-2008-1105
XREF	Secunia:30228
XREF	CWE:119

Plugin Information

Published: 2008/05/29, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
The remote Samba server appears to be :

  Samba 3.0.20-Debian
```

122058 - Samba < 3.4.0 Remote Code Execution Vulnerability

Synopsis

The remote Samba server is affected by a remote code execution vulnerability.

Description

The version of Samba running on the remote host is prior to 3.4.0. It is, therefore, affected by a remote code execution vulnerability in process.c due to a heap-based buffer overflow. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands via Batched / AndX request.

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://www.samba.org/samba/security/CVE-2012-0870.html

Solution

Upgrade to Samba version 3.4.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.9339

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	52103
CVE	CVE-2012-0870

Plugin Information

Published: 2019/02/08, Modified: 2019/10/31

Plugin Output

tcp/445/cifs

```
Installed version : 3.0.20-Debian
Fixed version     : 3.4.0
```

168018 - Samba < 4.15.12, 4.16.x < 4.16.7, and 4.17.x < 4.17.3 32-Bit Systems Buffer Overflow

Synopsis

The remote Samba server is potentially affected by a buffer overflow vulnerability

Description

The version of Samba running on the remote host is prior to 4.15.12, 4.16.x prior to 4.16.7, or 4.17.x prior to 4.17.3.

It is, therefore, potentially affected by a buffer overflow condition in the bundled Kerberos libraries due to a miss calculation of bytes to allocate for a buffer. An authenticated, remote attacker can exploit this, via a specially crafted ticket containing Privilege Attribute Certificates, to cause a denial of service condition or read beyond the memory bounds.

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.samba.org/samba/security/CVE-2022-42898.html

Solution

Upgrade to Samba version 4.15.12, 4.16.7, 4.17.3 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0171

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-42898
XREF	IAVA:2022-A-0495-S

Plugin Information

Published: 2022/11/21, Modified: 2023/10/03

Plugin Output

tcp/445/cifs

```
Installed version : 3.0.20-Debian
Fixed version     : 4.15.12
```

90509 - Samba Badlock Vulnerability

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists 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 who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0489

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	86002
CVE	CVE-2016-2118
XREF	CERT:813296

Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Nessus detected that the Samba Badlock patch has not been applied.
```

19704 - TWiki 'rev' Parameter Arbitrary Command Execution

Synopsis

The remote web server hosts a CGI application that is affected by an arbitrary command execution vulnerability.

Description

The version of TWiki running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

See Also

http://www.nessus.org/u?c70904f3

Solution

Apply the appropriate hotfix referenced in the vendor advisory.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.9517

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)

References

BID	14834
CVE	CVE-2005-2877

Exploitable With

Metasploit (true)

Plugin Information

Published: 2005/09/15, Modified: 2024/06/05

Plugin Output

tcp/80/www

```
Nessus was able to execute the command "id" using the
following request :

http://Epic-Metasploitable.epicode/twiki/bin/view/Main/TWikiUsers?rev=2%20%7cid%7c%7cecho%20


This produced the following truncated output (limited to 2 lines) :
------------------------------ snip ------------------------------
uid=33(www-data) gid=33(www-data) groups=33(www-data)

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

17210 - TWiki ImageGalleryPlugin Shell Command Injection

Synopsis

The remote web server hosts a CGI application that is affected by multiple vulnerabilities.

Description

According to its version number, the instance of TWiki running on the remote host is affected by a shell command injection vulnerability in the ImageGalleryPlugin component.

In addition, the wording of a 'robustness' patch released by the vendor indicates this version may be affected by other input validation issues. It should be noted that the patch may contain proactive security enhancements but they may not fix specific vulnerabilities.

See Also

https://seclists.org/fulldisclosure/2005/Feb/562

Solution

Apply the TWiki robustness patch referenced in the advisory.

Risk Factor

High

VPR Score

6.1

EPSS Score

0.0351

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	12637
BID	12638
CVE	CVE-2005-0516

Plugin Information

Published: 2005/02/24, Modified: 2024/06/05

Plugin Output

tcp/80/www

```
URL               : http://Epic-Metasploitable.epicode/twiki/bin/view
Installed version : 01 Feb 2003
Fixed version     : apply the referenced patch
```

36171 - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

Synopsis

The remote web server contains a PHP application that is affected by a code execution vulnerability.

Description

The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user-supplied input before using it to generate a config file for the application. This version is affected by the following vulnerabilities :

- The setup script inserts the unsanitized verbose server name into a C-style comment during config file generation.

- An attacker can save arbitrary data to the generated config file by altering the value of the 'textconfig' parameter during a POST request to config.php.

An unauthenticated, remote attacker can exploit these issues to execute arbitrary PHP code.

See Also

https://www.tenable.com/security/research/tra-2009-02

http://www.phpmyadmin.net/home_page/security/PMASA-2009-4.php

Solution

Upgrade to phpMyAdmin 3.1.3.2. Alternatively, apply the patches referenced in the project's advisory.

Risk Factor

High

VPR Score

6.7

EPSS Score

0.0294

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	34526
CVE	CVE-2009-1285
XREF	TRA:TRA-2009-02
XREF	SECUNIA:34727
XREF	CWE:94

Plugin Information

Published: 2009/04/16, Modified: 2022/04/11

Plugin Output

tcp/80/www

17814 - yaSSL 1.7.5 Buffer Overflow

Synopsis

Arbitrary code can be executed on the remote database server.

Description

The version of MySQL installed on the remote host reportedly allows a remote user to execute arbitrary code by exploiting a buffer overflow in yaSSL 1.7.5 or earlier.

See Also

https://bugs.mysql.com/bug.php?id=33814

https://www.securityfocus.com/archive/1/archive/1/485810/100/0/threaded

Solution

Upgrade to MySQL version 5.0.54a, 5.1.23, 6.0.4 or later.

Risk Factor

High

VPR Score

7.3

EPSS Score

0.9741

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)

References

BID	27140
CVE	CVE-2008-0226
CVE	CVE-2008-0227
XREF	CWE:119

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2012/01/16, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.0.55
```

83346 - .bash_history Files Disclosed via Web Server

Synopsis

The remote web server hosts what may be a publicly accessible .bash_history file.

Description

Nessus has detected that the remote web server hosts publicly available files whose contents may be indicative of a typical bash history. Such files may contain sensitive information that should not be disclosed to the public.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information, and that the files are only accessible to those with valid credentials.

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: 2015/05/12, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The following .bash_history files are available on the remote server :

  - /twiki/bin/search/Main/.bash_history
Note, this file is being flagged because you have set your scan to 'Paranoid'.
The contents of the detected file has not been inspected to see if it contains any of the common
 Linux commands one might expect to see in a typical .bash_history file.
  - /twiki/bin/oops/Main/WebHomemailto:webmasteryour/.bash_history
Note, this file is being flagged because you have set your scan to 'Paranoid'.
The contents of the detected file has not been inspected to see if it contains any of the common
 Linux commands one might expect to see in a typical .bash_history file.
  - /twiki/bin/view/Main/.bash_history
Note, this file is being flagged because you have set your scan to 'Paranoid'.
The contents of the detected file has not been inspected to see if it contains any of the common
 Linux commands one might expect to see in a typical .bash_history file.
```

48205 - Apache 2.2.x < 2.2.16 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 2.2.16. It is, therefore, potentially affected by multiple vulnerabilities :

- A denial of service vulnerability in mod_cache and mod_dav. (CVE-2010-1452)

- An information disclosure vulnerability in mod_proxy_ajp, mod_reqtimeout, and mod_proxy_http relating to timeout conditions. Note that this issue only affects Apache on Windows, Netware, and OS/2. (CVE-2010-2068)

Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See Also

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

https://issues.apache.org/bugzilla/show_bug.cgi?id=49246

https://bz.apache.org/bugzilla/show_bug.cgi?id=49417

http://www.nessus.org/u?ce8ac446

Solution

Upgrade to Apache version 2.2.16 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

3.6

EPSS Score

0.2873

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	40827
BID	41963
CVE	CVE-2010-1452
CVE	CVE-2010-2068
XREF	Secunia:40206

Plugin Information

Published: 2010/07/30, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.16
```

50070 - Apache 2.2.x < 2.2.17 Multiple Vulnerabilities

Synopsis

The remote web server may be affected by several issues.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.17. It is, therefore, affected by the following vulnerabilities :

- Errors exist in the bundled expat library that may allow an attacker to crash the server when a buffer is over- read when parsing an XML document. (CVE-2009-3720 and CVE-2009-3560)

- An error exists in the 'apr_brigade_split_line' function in the bundled APR-util library. Carefully timed bytes in requests result in gradual memory increases leading to a denial of service. (CVE-2010-1623) Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.17

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

Solution

Upgrade to Apache version 2.2.17 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

4.4

EPSS Score

0.8276

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	37203
BID	36097
BID	43673
CVE	CVE-2009-3560
CVE	CVE-2009-3720
CVE	CVE-2010-1623
XREF	Secunia:41701
XREF	CWE:119

Plugin Information

Published: 2010/10/20, Modified: 2018/06/29

Plugin Output

tcp/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.17
```

53896 - Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS

Synopsis

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

Description

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

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

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

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.18

http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18

http://securityreason.com/achievement_securityalert/98

Solution

Upgrade to Apache version 2.2.18 or later. Alternatively, ensure that the 'IndexOptions' configuration option is set to 'IgnoreClient'.

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

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

VPR Score

4.4

EPSS Score

0.9667

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	47820
CVE	CVE-2011-0419
XREF	Secunia:44574

Plugin Information

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

Plugin Output

tcp/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.18
```

56216 - Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS

Synopsis

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

Description

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

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

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.21

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

Solution

Upgrade to Apache version 2.2.21 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:N/A:L)

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.494

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	49616
CVE	CVE-2011-3348

Plugin Information

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

Plugin Output

tcp/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.21
```

57791 - Apache 2.2.x < 2.2.22 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

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

- When configured as a reverse proxy, improper use of the RewriteRule and ProxyPassMatch directives could cause the web server to proxy requests to arbitrary hosts.

This could allow a remote attacker to indirectly send requests to intranet servers.

(CVE-2011-3368, CVE-2011-4317)

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

- A format string handling error can allow the server to be crashed via maliciously crafted cookies.

(CVE-2012-0021)

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

(CVE-2012-0031)

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

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

Note that 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

EPSS Score

0.9702

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/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
```

```
    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

EPSS Score

0.1707

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/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
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

4.4

EPSS Score

0.5048

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/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
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

EPSS Score

0.3357

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/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.27
```

33477 - Apache 2.2.x < 2.2.9 Multiple Vulnerabilities (DoS, XSS)

Synopsis

The remote web server may be affected by several issues.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.9. It is, therefore, affected by multiple vulnerabilities :

- Improper handling of excessive forwarded interim responses may cause denial of service conditions in mod_proxy_http. (CVE-2008-2364)

- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer. (CVE-2007-6420)

Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2

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

Solution

Upgrade to Apache version 2.2.9 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

4.2

EPSS Score

0.221

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	27236
BID	29653
CVE	CVE-2007-6420
CVE	CVE-2008-2364
CVE	CVE-2007-6423
XREF	Secunia:30621
XREF	CWE:352
XREF	CWE:399

Plugin Information

Published: 2008/07/11, Modified: 2018/06/29

Plugin Output

tcp/80/www

```
Version source    : Server: Apache/2.2.8 (Ubuntu) DAV/2
Installed version : 2.2.8
Fixed version     : 2.2.9
```

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

EPSS Score

0.0027

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/80/www

```
URL               : http://Epic-Metasploitable.epicode/
Installed version : 2.2.8
Fixed version     : 2.4.54
```

57792 - Apache HTTP Server httpOnly Cookie Information Disclosure

Synopsis

The web server running on the remote host is affected by an information disclosure vulnerability.

Description

The version of Apache HTTP Server running on the remote host is affected by an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

See Also

http://fd.the-wildcat.de/apache_e36a9cf46c.php

http://www.nessus.org/u?e005199a

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

http://svn.apache.org/viewvc?view=revision&revision=1235454

Solution

Upgrade to Apache version 2.0.65 / 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

2.2

EPSS Score

0.5744

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

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

References

BID	51706
CVE	CVE-2012-0053
XREF	EDB-ID:18442

Plugin Information

Published: 2012/02/02, Modified: 2018/09/20

Plugin Output

tcp/80/www

```
Nessus verified this by sending a request with a long Cookie header :

GET / HTTP/1.1
Host: Epic-Metasploitable.epicode
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
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, */*

Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated) :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Size of a request header field exceeds server limit.<br />
<pre>
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
```

106232 - Apache ServerTokens Information Disclosure

Synopsis

The remote web server discloses information via HTTP headers.

Description

The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version, operating system, and module versions.

See Also

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

Solution

Change the Apache ServerTokens configuration value to 'Prod'

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: 2018/01/22, Modified: 2020/04/22

Plugin Output

tcp/80/www

```
The Apache server listening on port 80 contains
sensitive information in the HTTP Server field.

Server: Apache/2.2.8 (Ubuntu) DAV/2
```

12085 - Apache Tomcat Default Files

Synopsis

The remote web server contains default files.

Description

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

See Also

http://www.nessus.org/u?4cb3b4dd

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

Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

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: 2004/03/02, Modified: 2024/09/03

Plugin Output

tcp/8180/www

```
The following default files were found :

http://Epic-Metasploitable.epicode:8180/tomcat-docs/index.html

The server is not configured to return a custom page in the event of a client requesting a non-
existent resource.
This may result in a potential disclosure of sensitive information about the server to attackers.
```

11411 - Backup Files Disclosure

Synopsis

It is possible to retrieve file backups from the remote web server.

Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

See Also

http://www.nessus.org/u?8f3302c6

Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

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: 2003/03/17, Modified: 2023/07/10

Plugin Output

tcp/80/www

```
It is possible to read the following backup files :

  - File                  : /twiki/bin/view/Main/WebHome~
    URL                   : http://Epic-Metasploitable.epicode/twiki/bin/view/Main/WebHome~
    Response body snippet :
    ------------------------------ snip ------------------------------
    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "ht [...]
    <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
    <head>
    <title> TWiki . Main . WebHome   </title>
    <meta http-equiv="Content-Type" content="text/html; charset=ISO-88 [...]
    <base href="http://Epic-Metasploitable.epicode/twiki/bin/view/Main [...]
    </head>
    <body bgcolor="#ffffff">
    <a name="PageTop"></a>
    <form name="main" action="/twiki/bin/view/Main/WebHome">
```

```
    [...]
    ------------------------------ snip ------------------------------

- File                  : /twiki/bin/search/Main/SearchResult~
  URL                   : http://Epic-Metasploitable.epicode/twiki/bin/search/Main/SearchResult~
  Response body snippet :
  ------------------------------ snip ------------------------------
  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "ht [...]
  <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
  <head>
  <title>TWiki . Main (search result)</title>
  <meta http-equiv="Content-Type" content="text/html; charset=ISO-88 [...]
  <meta name="robots" content="noindex" />
  <base href="http://Epic-Metasploitable.epicode/twiki/bin/view/Main [...]
  </head>
  <body bgcolor="#ffffff">
  <a name="PageTop"></a>
  [...]
  ------------------------------ snip ------------------------------
```

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/80/www

```
The following directories are browsable :

http://Epic-Metasploitable.epicode/dav/
http://Epic-Metasploitable.epicode/dvwa/dvwa/
http://Epic-Metasploitable.epicode/dvwa/dvwa/css/
http://Epic-Metasploitable.epicode/dvwa/dvwa/images/
http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/
http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/
http://Epic-Metasploitable.epicode/dvwa/dvwa/js/
http://Epic-Metasploitable.epicode/mutillidae/documentation/
http://Epic-Metasploitable.epicode/mutillidae/styles/
http://Epic-Metasploitable.epicode/mutillidae/styles/ddsmoothmenu/
```

```
http://Epic-Metasploitable.epicode/test/
http://Epic-Metasploitable.epicode/test/testoutput/
```

44136 - CGI Generic Cookie Injection Scripting

Synopsis

The remote web server is prone to cookie injection attacks.

Description

The remote web server hosts at least one CGI script that fails to adequately sanitize request strings with malicious JavaScript.

By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible to launch a 'session fixation' attack using this mechanism.

Please note that :

- Nessus did not check if the session fixation attack is feasible.

- This is not the only vector of session fixation.

See Also

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

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

http://www.acros.si/papers/session_fixation.pdf

http://projects.webappsec.org/w/page/13246960/Session%20Fixation

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

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:472
XREF	CWE:642
XREF	CWE:715
XREF	CWE:722

Plugin Information

Published: 2010/01/25, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to cookie manipulation :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=<script>document.cookie="testatir=7317;"</script>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<script>document.cookie="t
estatir=7317;"</script>">Toggle Hints</a></td><td><a href="./index.
php?do=toggle-security&page=<script>document.cookie="testatir=7317;"</sc
ript>">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?page=<script>document.cookie="testatir=7317;"</scr
ipt>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<script>document.cookie="t
estatir=7317;"</script>">Toggle Hints</a></td><td><a href="./index.
php?do=toggle-security&page=<script>document.cookie="testatir=7317;"</sc
ript>">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

/mutillidae/index.php?do=toggle-hints&page=<script>document.cookie="test
atir=7317;"</script>&username=anonymous

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<script>document.cookie="t
estatir=7317;"</script>">Toggle Hints</a></td><td><a href="./index.
php?do=toggle-security&page=<script>document.cookie="testatir=7317;"</sc
ript>">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------
```

49067 - CGI Generic HTML Injections (quick test)

Synopsis

The remote web server may be prone to HTML injections.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML to be executed in a user's browser within the security context of the affected site.

The remote web server may be vulnerable to IFRAME injections or cross-site scripting attacks :

- IFRAME injections allow 'virtual defacement' that might scare or anger gullible users. Such injections are sometimes implemented for 'phishing' attacks.

- XSS are extensively tested by four other scripts.

- Some applications (e.g. web forums) authorize a subset of HTML without any ill effect. In this case, ignore this warning.

See Also

http://www.nessus.org/u?602759bc

Solution

Either restrict access to the vulnerable application or contact the vendor for an update.

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:80
XREF	CWE:86

Plugin Information

Published: 2010/09/01, Modified: 2021/01/19

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to HTML injection :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=%00<<<<"dolrai%20>>>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=.<<<<"dolrai >>>">Toggle H
ints</a></td><td><a href="./index.php?do=toggle-security&page=.<<<<
"dolrai >>>">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

+ The 'template' parameter of the /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company CGI :

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template=%00<<<
<"dolrai%20>>>

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file .<<<<"dolrai >>>.tmpl not found or template directory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?page=%00<<<<"dolrai%20>>>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=.<<<<"dolrai >>>">Toggle H
ints</a></td><td><a href="./index.php?do=toggle-security&page=.<<<<
"dolrai >>>">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

/mutillidae/index.php?do=toggle-hints&page=%00<<<<"dolrai%20>>>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=%00<<<<"dolrai%20>>>">Togg
le Hints</a></td><td><a href="./index.php?do=toggle-security&page=%
00<<<<"dolrai%20>>>">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
----------------- [...]
```

42872 - CGI Generic Local File Inclusion (2nd pass)

Synopsis

Arbitrary code may be run on this server.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a local file and disclose its contents, or even execute arbitrary code on the remote host.

See Also

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

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	CWE:73
XREF	CWE:78
XREF	CWE:98
XREF	CWE:473
XREF	CWE:632
XREF	CWE:714
XREF	CWE:727
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/11/19, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
-------- request --------
GET /mutillidae/index.php?page=<IMG%20SRC="javascript:alert(104);"> HTTP/1.1
Host: Epic-Metasploitable.epicode
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, */*
------------------------

-------- output --------
<!-- Begin Content -->
<br />
<b>Warning</b>:  include(&lt;IMG SRC=&quot;javascript:alert(104);&quot;&
gt;) [<a href='function.include'>function.include</a>]: failed to open s
tream: No such file or directory in <b>/var/www/mutillidae/index.php</b>
 on line <b>469</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------

-------- request --------
POST /mutillidae/index.php HTTP/1.1
Host: Epic-Metasploitable.epicode
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Cookie: showhints=1; PHPSESSID=7c7924f6be56276a14406ded8989c965
Content-Length: 74
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, */*
do=toggle-hints&page=<IMG SRC="javascript:alert(104);">&username=anonymous------------------------

-------- output --------
<!-- Begin Content -->
<br />
<b>Warning</b>:  include(&lt;IMG SRC=&quot;javascript:alert(104);&quot;&
gt;) [<a href='function.include'>function.include</a>]: failed to open s
tream: No such file or directory in <b>/var/www/mutillidae/index.php</b>
 on line <b>469</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------

-------- request --------
GET /mutillidae/?page=<IMG%20SRC="javascript:alert(104);"> HTTP/1.1
Host: Epic-Metasploitable.epicode
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connect [...]
```

39467 - CGI Generic Path Traversal

Synopsis

Arbitrary files may be accessed or executed on the remote host.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings and are affected by directory traversal or local files inclusion vulnerabilities.

By leveraging this issue, an attacker may be able to read arbitrary files on the web server or execute commands.

See Also

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

http://cwe.mitre.org/data/definitions/22.html

http://projects.webappsec.org/w/page/13246952/Path%20Traversal

http://projects.webappsec.org/w/page/13246949/Null%20Byte%20Injection

http://www.nessus.org/u?4de3840d

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address path traversal flaws.

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)

References

XREF	OWASP:OWASP-AZ-001
XREF	CWE:21
XREF	CWE:22
XREF	CWE:632
XREF	CWE:715
XREF	CWE:723

XREF	CWE:813
XREF	CWE:928
XREF	CWE:932

Plugin Information

Published: 2009/06/19, Modified: 2022/04/07

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to directory traversal :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=../../../../../../../../../etc/passwd%00index.html

-------- output --------
<blockquote>
<!-- Begin Content -->
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
------------------------

+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?page=../../../../../../../../../etc/passwd%00index.ht
ml

-------- output --------
<blockquote>
<!-- Begin Content -->
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
------------------------
```

46195 - CGI Generic Path Traversal (extended test)

Synopsis

Arbitrary files may be accessed or executed on the remote host.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings and are affected by directory traversal or local file inclusion vulnerabilities.

By leveraging this issue, an attacker may be able to read arbitrary files on the web server or execute commands.

See Also

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

http://projects.webappsec.org/w/page/13246952/Path%20Traversal

http://projects.webappsec.org/w/page/13246949/Null%20Byte%20Injection

http://www.nessus.org/u?70f7aa09

Solution

Either restrict access to the vulnerable application or contact the vendor for an update.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	OWASP:OWASP-AZ-001
XREF	CWE:21
XREF	CWE:22
XREF	CWE:632
XREF	CWE:715
XREF	CWE:723
XREF	CWE:813
XREF	CWE:928
XREF	CWE:932

Plugin Information

Published: 2010/04/30, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to directory traversal (extended test) :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=./.././../../../../../../../../../etc/passwd

-------- output --------
<blockquote>
<!-- Begin Content -->
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
------------------------
```

46194 - CGI Generic Path Traversal (write test)

Synopsis

Arbitrary files may be modified on the remote host.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings and are affected by directory traversal or local file inclusion vulnerabilities.

By leveraging this issue, an attacker may be able to modify arbitrary files on the web server or execute commands.

Due to the way this flaw is tested, this script is prone to false positives.

See Also

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

http://cwe.mitre.org/data/definitions/22.html

http://projects.webappsec.org/w/page/13246952/Path%20Traversal

http://projects.webappsec.org/w/page/13246949/Null%20Byte%20Injection

http://www.nessus.org/u?70f7aa09

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	OWASP:OWASP-AZ-001

Plugin Information

Published: 2010/04/30, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to directory traversal (write access) :

+ The 'nocache' parameter of the /phpMyAdmin/phpmyadmin.css.php CGI :

/phpMyAdmin/phpmyadmin.css.php?token=cf11a17fc0ebb6468a05dbea2f5c55c5&js
_frame=right&nocache=2457687151../../../../../../../../../../tmp

-------- output --------
/* general tags */
html {
    font-size: 84%;
}

-------- vs --------
/* general tags */
html {
    font-size: 82%;
}
------------------------

/phpMyAdmin/phpmyadmin.css.php?token=cf11a17fc0ebb6468a05dbea2f5c55c5&js
_frame=right&nocache=2457687151../../../../../../../../../../tmp {2}

-------- output --------
/* general tags */
html {
    font-size: 84%;
}

-------- vs --------
/* general tags */
html {
    font-size: 82%;
}
------------------------


Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to directory traversal (write access) :

+ The 'lang' parameter of the /phpMyAdmin/index.php CGI :

/phpMyAdmin/index.php [pma_password=&db=&token=cf11a17fc0ebb6468a05dbea2
f5c55c5&table=&server=1&pma_username=&lang=en-utf-8../../../../../../../
../../../windows/system32/config/sam]

-------- output --------
    <link rel="shortcut icon" href="./favicon.ico" type="image/x-i [...]
    <title>phpMyAdmin </title>
    <link rel="stylesheet" type="text/css" href="phpmyadmin.css.php?toke
n=98e3ea6e7000660d06b6a266bc60df91&amp;js_frame=right&amp;nocache=245768
7151" />
    <link rel="stylesheet" type="text/css" href="print.css" media= [...]
    <meta name="robots" content="noindex,nofollow" />
-------- vs --------
    <link rel="shortcut icon" href="./favicon.ico" type="image/x-i [...]
    <title>phpMyAdmin </title>
    <link rel="stylesheet" type="text/css" href="phpmyadmin.css.php?toke
n=98e3ea6e7000660d06b6a266bc60df91&amp;js_frame=right&amp;nocache=245768
7233" />
    <link rel="stylesheet" type="text/css" href="print.css" media= [...]
    <meta name="robots" content="noindex,nofollow" />
------------------------
```

```
+ [...]
```

46196 - CGI Generic XML Injection

Synopsis

A CGI application hosted on the remote web server is potentially prone to an XML injection attack.

Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access a SOAP back-end.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

Exploitation of XML injections is usually far from trivial.

See Also

http://www.nessus.org/u?5691cc8c

Solution

Modify the affected CGI scripts so that they properly escape arguments, especially XML tags and special characters (angle brackets and slashes).

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	OWASP:OWASP-DV-008
XREF	CWE:91
XREF	CWE:713
XREF	CWE:722
XREF	CWE:727
XREF	CWE:810
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2010/04/30, Modified: 2024/06/14

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to XML injection :

+ The 'nocache' parameter of the /phpMyAdmin/phpmyadmin.css.php CGI :

/phpMyAdmin/phpmyadmin.css.php?token=cf11a17fc0ebb6468a05dbea2f5c55c5&js
_frame=right&nocache=2457687151</%20foo>

-------- output --------
/* general tags */
html {
    font-size: 84%;
}

-------- vs --------
/* general tags */
html {
    font-size: 82%;
}
------------------------

/phpMyAdmin/phpmyadmin.css.php?token=cf11a17fc0ebb6468a05dbea2f5c55c5&js
_frame=right&nocache=2457687151</%20foo> {2}

-------- output --------
/* general tags */
html {
    font-size: 84%;
}

-------- vs --------
/* general tags */
html {
    font-size: 82%;
}
------------------------
```

47831 - CGI Generic XSS (comprehensive test)

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. These XSS are likely to be 'non-persistent' or 'reflected'.

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

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:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:84
XREF	CWE:85
XREF	CWE:86
XREF	CWE:87
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692

XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

Published: 2010/07/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to cross-site scripting (comprehensive test) :

+ The 'template' parameter of the /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company CGI :

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template=>>>>>>
>>>>foo"bar'207<<<<<

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file >>>>>>>>>>foo"bar'207<<<<<.tmpl not found or template dire
ctory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=<%20script%20>%20alert(204);%20</%20script%20>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=< script > alert(204); </
script >">Toggle Hints</a></td><td><a href="./index.php?do=toggle-s
ecurity&page=< script > alert(204); </ script >">Toggle Security</a></td
>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------
```

55903 - CGI Generic XSS (extended patterns)

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts one or more CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. These XSS vulnerabilities are likely to be 'non-persistent' or 'reflected'.

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

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:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:86
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725

XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

Published: 2011/08/03, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to cross-site scripting (extended patterns) :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=504%20onerror="alert(504);

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=504 onerror="alert(504);">
Toggle Hints</a></td><td><a href="./index.php?do=toggle-security&pa
ge=504 onerror="alert(504);">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?page=504%20onerror="alert(504);

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=504 onerror="alert(504);">
Toggle Hints</a></td><td><a href="./index.php?do=toggle-security&pa
ge=504 onerror="alert(504);">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://Epic-Metasploitable.epicode/mutillidae/?page=504%20onerror="alert(504);


Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to cross-site scripting (extended patterns) :

/mutillidae/index.php [do=toggle-hints&page=504 onerror="alert(504);]

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=504 onerror="alert(504);">
```

```
Toggle Hints</a></td><td><a href="./index.php?do=toggle-security&pa
ge=504 onerror="alert(504);">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------
```

39466 - CGI Generic XSS (quick test)

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.

These XSS are likely to be 'non persistent' or 'reflected'.

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

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:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:86
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692
XREF	CWE:712
XREF	CWE:722

XREF	CWE:725
XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

Published: 2009/06/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to cross-site scripting (quick test) :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=<IMG%20SRC="javascript:alert(104);">

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<IMG SRC="javascript:alert
(104);">">Toggle Hints</a></td><td><a href="./index.php?do=toggle-s
ecurity&page=<IMG SRC="javascript:alert(104);">">Toggle Security</a></td
>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

+ The 'template' parameter of the /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company CGI :

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template="><obj
ect%20type="text/html"%20data="http://www.example.com/include.html"></ob
ject>

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file "><object type="text/html" data="http://www.example.com/in
clude.html"></object>.tmpl not found or template directory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?page=<IMG%20SRC="javascript:alert(104);">

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<IMG SRC="javascript:alert
(104);">">Toggle Hints</a></td><td><a href="./index.php?do=toggle-s
ecurity&page=<IMG SRC="javascript:alert(104);">">Toggle Security</a></td
>
<td><a href="set-up-database.php">Reset DB</a></td>
```

```
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------


Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to cross-site scripting (quick test) :

/mutillidae/index.php [do=toggle-hints&page=<IMG SRC="javascript:alert(1
04);">&username [...]
```

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

EPSS Score

0.0225

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/80/www

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

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

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

Nessus sent the following TRACE request : \n\n------------------------------ snip
 ------------------------------\nTRACE /Nessus1089077373.html HTTP/1.1
Connection: Close
Host: Epic-Metasploitable.epicode
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: Sun, 09 Feb 2025 23:47:40 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1089077373.html HTTP/1.1
Connection: Keep-Alive
```

```
Host: Epic-Metasploitable.epicode
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
```

89998 - ISC BIND 9 Multiple DoS

Synopsis

The remote name server is affected by multiple denial of service vulnerabilities.

Description

According to its self-reported version number, the instance of ISC BIND running on the remote name server is affected by multiple denial of service vulnerabilities :

- A denial of service vulnerability exists in files sexpr.c and alist.c when handling control channel packets. An unauthenticated, remote attacker can exploit this, via crafted packets sent to the control channel (rndc) interface, to cause an assertion failure and daemon exit. (CVE-2016-1285)

- A denial of service vulnerability exists in resolver.c when DNS cookies are enabled. An unauthenticated, remote attacker can exploit this, via a malformed cookie with more than one cookie option, to cause an INSIST assertion failure and daemon exit. (CVE-2016-2088)

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://kb.isc.org/docs/aa-01352

https://kb.isc.org/article/AA-01362/

Solution

Upgrade to ISC BIND version 9.9.8-P4 / 9.9.8-S6 / 9.10.3-P4 or later.

Note that version 9.9.8-S6 is a preview version of BIND provided exclusively to ISC Support customers. Additionally, the fix for CVE-2016-2088 is only available in version 9.10.3-P4.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.8396

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-1285
CVE	CVE-2016-2088

Plugin Information

Published: 2016/03/17, Modified: 2019/11/20

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.8-P4 / 9.9.8-S6 / 9.10.3-P4
```

154662 - ISC BIND 9.3.0 < 9.11.36 / 9.9.3-S1 < 9.11.36-S1 / 9.12.0 < 9.16.22 / 9.16.8-S1 < 9.16.22-S1 / 9.17.0 < 9.17.19 Vulnerability (CVE-2021-25219)

Synopsis

The remote name server is affected by a vulnerability vulnerability.

Description

The version of ISC BIND installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the CVE-2021-25219 advisory.

- In BIND 9.3.0 -> 9.11.35, 9.12.0 -> 9.16.21, and versions 9.9.3-S1 -> 9.11.35-S1 and 9.16.8-S1 ->

9.16.21-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.18 of the BIND 9.17 development branch, exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing. (CVE-2021-25219)

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://kb.isc.org/v1/docs/CVE-2021-25219

Solution

Upgrade to ISC BIND version 9.11.36 / 9.11.36-S1 / 9.16.22 / 9.16.22-S1 / 9.17.19 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:N/A:L)

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.006

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-2021-25219
XREF	IAVA:2021-A-0525-S

Plugin Information

Published: 2021/10/28, Modified: 2022/09/27

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.36
```

165312 - ISC BIND 9.9.3-S1 < 9.16.33-S1 / 9.0.0 < 9.16.33 / 9.16.8-S1 < 9.16.33-S1 / 9.18.0 < 9.18.7 / 9.19.0 < 9.19.5 Vulnerability (cve-2022-2795)

Synopsis

The remote name server is affected by a vulnerability vulnerability.

Description

The version of ISC BIND installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the cve-2022-2795 advisory.

- By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service.

(CVE-2022-2795)

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://kb.isc.org/v1/docs/cve-2022-2795

Solution

Upgrade to ISC BIND version 9.16.33 / 9.16.33-S1 / 9.18.7 / 9.19.5 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:N/A:L)

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0035

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-2022-2795
XREF	IAVA:2022-A-0387-S
XREF	IAVA:2023-A-0500-S

Plugin Information

Published: 2022/09/22, Modified: 2024/02/16

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.16.33
```

139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

Synopsis

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

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.

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://kb.isc.org/docs/cve-2020-8622

Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-8622
XREF	IAVA:2020-A-0385-S

Plugin Information

Published: 2020/08/27, Modified: 2021/06/03

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.22, 9.16.6, 9.17.4 or later
```

92493 - ISC BIND 9.x < 9.9.9-P2 / 9.10.x < 9.10.4-P2 / 9.11.0a3 < 9.11.0b2 lwres Query DoS

Synopsis

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

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is 9.x prior to 9.9.9-P2, 9.10.x prior to 9.10.4-P2, or 9.11.0a3 prior to 9.11.0b2. It is, therefore, affected by an error in the lightweight resolver (lwres) protocol implementation when resolving a query name that, when combined with a search list entry, exceeds the maximum allowable length. An unauthenticated, remote attacker can exploit this to cause a segmentation fault, resulting in a denial of service condition. This issue occurs when lwresd or the the named 'lwres' option is enabled.

See Also

https://kb.isc.org/article/AA-01393

Solution

Upgrade to ISC BIND version 9.9.8-P3 / 9.9.8-S4 / 9.10.3-P3 or later.

Note that BIND 9 version 9.9.9-S3 is available exclusively for eligible ISC Support customers.

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:N/A:H)

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.8997

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2016-2775
XREF	IAVA:2017-A-0004

Plugin Information

Published: 2016/07/21, Modified: 2019/11/14

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.9.9-P2
```

119264 - ISC BIND 9.x.x < 9.11.5 / 9.12.x < 9.12.3 Policy-Bypass Record Update Vulnerability

Synopsis

The remote name server is affected by a policy bypass which enables an unauthorized record update vulnerability.

Description

According to its self-reported version number, the instance of ISC 9.x.x prior to 9.11.5, or 9.12.x prior to 9.12.3. It is, therefore, affected by a policy bypass record update vulnerability.

See Also

https://kb.isc.org/docs/cve-2018-5741

Solution

Upgrade to ISC BIND version 9.11.5 / 9.12.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0056

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	105379
CVE	CVE-2018-5741

Plugin Information

Published: 2018/11/28, Modified: 2019/11/01

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.5
```

62355 - ISC BIND Cache Update Policy Deleted Domain Name Resolving Weakness

Synopsis

The remote name server may be affected by a DNS integrity vulnerability.

Description

According to its self-reported version number, the remote installation of BIND will continue to allow revoked domain names to be resolved due to an issue related to the cache update policy. Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

See Also

http://www.nessus.org/u?38f47769

https://www.isc.org/software/bind/advisories/cve-2012-1033

http://ftp.isc.org/isc/bind9/9.6-ESV-R6/CHANGES

http://ftp.isc.org/isc/bind9/9.7.5/CHANGES

http://ftp.isc.org/isc/bind9/9.8.2/CHANGES

http://ftp.isc.org/isc/bind9/9.9.0/CHANGES

Solution

Upgrade to BIND 9.6-ESV-R6 / 9.7.5 / 9.8.2 / 9.9.0 or later.

Risk Factor

Medium

VPR Score

3.4

EPSS Score

0.0205

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)

References

BID	51898
CVE	CVE-2012-1033
XREF	CERT:542123

Plugin Information

Published: 2012/09/27, Modified: 2018/06/27

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.6-ESV-R6
```

136808 - ISC BIND Denial of Service

Synopsis

The remote name server is affected by an assertion failure vulnerability.

Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.

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://kb.isc.org/docs/cve-2020-8617

Solution

Upgrade to the patched release most closely related to your current version of BIND.

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:N/A:H)

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.9724

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-8617
XREF	IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/22, Modified: 2023/03/23

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.19
```

40422 - ISC BIND Dynamic Update Message Handling Remote DoS

Synopsis

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

Description

The version of BIND installed on the remote host suggests that it suffers from a denial of service vulnerability, which may be triggered by sending a malicious dynamic update message to a zone for which the server is the master, even if that server is not configured to allow dynamic updates.

Note that Nessus obtained the version by sending a special DNS request for the text 'version.bind' in the domain 'chaos', the value of which can be and sometimes is tweaked by DNS administrators.

See Also

http://www.nessus.org/u?8662ded2

Solution

Upgrade to BIND 9.4.3-P3 / 9.5.1-P3 / 9.6.1-P3 or later.

Risk Factor

Medium

VPR Score

5.1

EPSS Score

0.955

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

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

References

BID	35848
CVE	CVE-2009-0696
XREF	CERT:725188

XREF CWE:16

Exploitable With

Core Impact (true)

Plugin Information

Published: 2009/07/29, Modified: 2018/06/27

Plugin Output

udp/53/dns

106679 - ISC BIND Zone Data Denial of Service

Synopsis

The remote name server is affected by a memory exhaustion vulnerability

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is affected by a memory exhaustion vulnerability. A server is potentially vulnerable if it accepts zone data from another source, as no limit is currently placed on zone data size.

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://kb.isc.org/article/AA-01390

Solution

Follow guidance provided by ISC advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0179

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-6170

Plugin Information

Published: 2018/02/08, Modified: 2018/06/29

Plugin Output

tcp/53/dns

```
Installed version : 9.4.2
```

56283 - Linux Kernel TCP Sequence Number Generation Security Weakness

Synopsis

It may be possible to predict TCP/IP Initial Sequence Numbers for the remote host.

Description

The Linux kernel is prone to a security weakness related to TCP sequence number generation. Attackers can exploit this issue to inject arbitrary packets into TCP sessions using a brute-force attack.

An attacker may use this vulnerability to create a denial of service condition or a man-in-the-middle attack.

Note that this plugin may fire as a result of a network device (such as a load balancer, VPN, IPS, transparent proxy, etc.) that is vulnerable and that re-writes TCP sequence numbers, rather than the host itself being vulnerable.

See Also

https://lwn.net/Articles/455135/

http://www.nessus.org/u?62a845fa

Solution

Contact the OS vendor for a Linux kernel update / patch.

Risk Factor

Medium

VPR Score

5.2

EPSS Score

0.0096

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	49289

CVE CVE-2011-3188

Plugin Information

Published: 2011/09/23, Modified: 2019/03/06

Plugin Output

tcp/0

42899 - MySQL 5.0 < 5.0.88 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL 5.0 installed on the remote host is earlier than 5.0.88. It is, therefore, potentially affected by the following vulnerabilities :

- MySQL clients linked against OpenSSL are vulnerable to man-in-the-middle attacks. (Bug #47320)

- The GeomFromWKB() function can be manipulated to cause a denial of service. (Bug #47780)

- Specially crafted SELECT statements containing sub- queries in the WHERE clause can cause the server to crash. (Bug #48291)

- It is possible to bypass access restrictions when the data directory contains a symbolic link to a different file system. (Bug #39277)

See Also

https://bugs.mysql.com/bug.php?id=47320

https://bugs.mysql.com/bug.php?id=47780

https://bugs.mysql.com/bug.php?id=48291

https://bugs.mysql.com/bug.php?id=39277

http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html

Solution

Upgrade to MySQL 5.0.88 or later.

Risk Factor

Medium

VPR Score

6.7

EPSS Score

0.1

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

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

References

BID	37076
BID	37297
BID	38043
CVE	CVE-2012-4452
CVE	CVE-2009-4019
CVE	CVE-2009-4028
CVE	CVE-2008-7247
XREF	Secunia:37372
XREF	CWE:20
XREF	CWE:59

Plugin Information

Published: 2009/11/25, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.0.88
```

57604 - MySQL 5.0 < 5.0.95 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL 5.0 installed on the remote host is earlier than 5.0.95. Such versions are affected by multiple vulnerabilities. Details are not public yet.

See Also

http://www.nessus.org/u?1ae3b967

http://www.nessus.org/u?abcc17ed

Solution

Upgrade to MySQL version 5.0.95 or later.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.0096

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	51502
BID	51505
BID	51509
BID	51515
BID	51520

BID	51524
BID	51526
CVE	CVE-2012-0075
CVE	CVE-2012-0087
CVE	CVE-2012-0101
CVE	CVE-2012-0102
CVE	CVE-2012-0114
CVE	CVE-2012-0484
CVE	CVE-2012-0490

Plugin Information

Published: 2012/01/19, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.0.95
```

17833 - MySQL < 5.0.54 / 5.1.23 / 6.0.4 Denial of Service

Synopsis

The remote database is vulnerable to a denial fo service attack.

Description

The version of MySQL installed on the remote host is older than 5.0.54, 5.1.23 or 6.0.4.

A remote attacker could crash the server by exploiting a flaw in InnoDB code.

See Also

https://bugs.mysql.com/bug.php?id=32125

Solution

Upgrade to MySQL version 5.0.54 / 5.1.23 / 6.0.4 or later.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.0974

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	26353
CVE	CVE-2007-5925
XREF	CWE:20

Plugin Information

Published: 2012/01/18, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.0.54
```

17812 - MySQL < 5.0.88 / 5.1.42 / 5.5.0 / 6.0.14 MyISAM CREATE TABLE Privilege Check Bypass

Synopsis

The remote database server allows a local user to circumvent privileges.

Description

The version of MySQL installed on the remote host is earlier than 5.0.88 / 5.1.42 / 5.5.0 / 6.0.14 and thus reportedly allows a local user to circumvent privileges through creation of MyISAM tables using the 'DATA DIRECTORY' and 'INDEX DIRECTORY' options to overwrite existing table files in the application's data directory. This is the same flaw as CVE-2008-2079, which was not completely fixed.

See Also

https://bugs.mysql.com/bug.php?id=32167?

Solution

Upgrade to MySQL version 5.0.88 / 5.1.42 / 5.5.0 / 6.0.14 or later.

Risk Factor

Medium

VPR Score

5.5

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29106
CVE	CVE-2008-4097
XREF	CWE:264

Plugin Information

Published: 2012/01/16, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.0.88
```

17834 - MySQL < 5.0.92 Multiple Denial of Service

Synopsis

The remote database server is vulnerable to multiple denial of service attacks.

Description

The version of MySQL installed on the remote host is older than 5.0.92. As such, it reportedly is prone to multiple denial of service attacks :

- The improper handling of type errors during argument evaluation in extreme-value functions, e.g., 'LEAST()'

or 'GREATEST()' causes server crashes. (CVE-2010-3833)

- Remote authenticated attackers could crash the server.

(CVE-2010-3834 & CVE-2010-3836)

- The use of 'GROUP_CONCAT()' and 'WITH ROLLUP' caused server crashes. (CVE-2010-3837)

- The use of an intermediate temporary table and queries containing calls to 'GREATEST()' or 'LEAST()', having a list of both numeric and 'LONGBLOB' arguments, caused server crashes. (CVE-2010-3838)

See Also

https://bugs.mysql.com/bug.php?id=55826

https://bugs.mysql.com/bug.php?id=54476

https://bugs.mysql.com/bug.php?id=54461

http://dev.mysql.com/doc/refman/5.0/en/news-5-0-92.html

https://bugzilla.redhat.com/show_bug.cgi?id=640751

Solution

Upgrade to MySQL version 5.0.92 or later.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.0798

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	43676
CVE	CVE-2010-3833
CVE	CVE-2010-3834
CVE	CVE-2010-3836
CVE	CVE-2010-3837
CVE	CVE-2010-3838

Plugin Information

Published: 2012/01/18, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.0.92
```

64503 - MySQL Binary Log SQL Injection

Synopsis

The database server running on the remote host has multiple SQL injection vulnerabilities.

Description

The version of MySQL installed on the remote host is earlier than 5.5.33 / 5.6.x earlier than 5.6.13 and is, therefore, potentially affected by multiple SQL injection vulnerabilities. User-supplied identifiers are not properly quoted before being written into the binary log. An attacker with a valid account and privileges to modify data could exploit this to modify tables that they should not have access to.

See Also

http://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-33.html

https://dev.mysql.com/doc/relnotes/mysql/5.6/en/news-5-6-13.html

https://mariadb.atlassian.net/browse/MDEV-382

https://www.openwall.com/lists/oss-security/2012/09/11/4

http://www.nessus.org/u?8f7e56e9

Solution

Upgrade to MySQL version 5.5.33 / 5.6.13 or later.

Risk Factor

Medium

VPR Score

5.9

EPSS Score

0.0015

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	55498
CVE	CVE-2012-4414

Plugin Information

Published: 2013/02/08, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.5.33 / 5.6.13
```

46702 - MySQL Community Server < 5.1.47 / 5.0.91 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL Community Server installed on the remote host is earlier than 5.1.47 / 5.0.91 and is, therefore, potentially affected by the following vulnerabilities :

- The server may continue reading packets indefinitely if it receives a packet larger than the maximum size of one packet, which could allow an unauthenticated, remote attacker to consume a high level of CPU and bandwidth. (Bug #50974)

- Using an overly long table name argument to the 'COM_FIELD_LIST' command, an authenticated user can overflow a buffer and execute arbitrary code on the affected host. (Bug #53237)

- Using a specially crafted table name argument to 'COM_FIELD_LIST', an authenticated user can bypass almost all forms of checks for privileges and table- level grants. (Bug #53371)

See Also

https://bugs.mysql.com/bug.php?id=50974

https://bugs.mysql.com/bug.php?id=53237

https://bugs.mysql.com/bug.php?id=53371

http://dev.mysql.com/doc/refman/5.0/en/news-5-0-91.html

http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html

Solution

Upgrade to MySQL Community Server 5.1.47 / 5.0.91 or later.

Risk Factor

Medium

VPR Score

7.4

EPSS Score

0.8863

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	40100
BID	40106
BID	40109
CVE	CVE-2010-1848
CVE	CVE-2010-1849
CVE	CVE-2010-1850

Exploitable With

CANVAS (true)

Plugin Information

Published: 2010/05/24, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.0.91
```

44079 - OpenSSH < 4.9 'ForceCommand' Directive Bypass

Synopsis

The remote SSH service is affected by a security bypass vulnerability.

Description

According to its banner, the version of OpenSSH installed on the remote host is earlier than 4.9. It may allow a remote, authenticated user to bypass the 'sshd_config' 'ForceCommand' directive by modifying the '.ssh/rc' session file.

See Also

https://www.openssh.com/txt/release-4.9

Solution

Upgrade to OpenSSH version 4.9 or later.

Risk Factor

Medium

VPR Score

6.1

EPSS Score

0.0521

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	28531
CVE	CVE-2008-1657
XREF	CWE:264

Plugin Information

Published: 2011/10/04, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 4.9
```

44065 - OpenSSH < 5.2 CBC Plaintext Disclosure

Synopsis

The SSH service running on the remote host has an information disclosure vulnerability.

Description

The version of OpenSSH running on the remote host has an information disclosure vulnerability. A design flaw in the SSH specification could allow a man-in-the-middle attacker to recover up to 32 bits of plaintext from an SSH-protected connection in the standard configuration. An attacker could exploit this to gain access to sensitive information.

See Also

http://www.nessus.org/u?4984aeb9

http://www.openssh.com/txt/cbc.adv

http://www.openssh.com/txt/release-5.2

Solution

Upgrade to OpenSSH 5.2 or later.

Risk Factor

Medium

VPR Score

6.5

EPSS Score

0.6016

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563

XREF CWE:200

Plugin Information

Published: 2011/09/27, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 5.2
```

85382 - OpenSSH < 7.0 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.0. It is, therefore, affected by the following vulnerabilities :

- A security bypass vulnerability exists in the kbdint_next_device() function in file auth2-chall.c that allows the circumvention of MaxAuthTries during keyboard-interactive authentication. A remote attacker can exploit this issue to force the same authentication method to be tried thousands of times in a single pass by using a crafted keyboard-interactive 'devices'

string, thus allowing a brute-force attack or causing a denial of service. (CVE-2015-5600)

- A security bypass vulnerability exists in sshd due to improper handling of username data in MONITOR_REQ_PAM_INIT_CTX requests. A local attacker can exploit this, by sending a MONITOR_REQ_PWNAM request, to conduct an impersonation attack. Note that this issue only affects Portable OpenSSH. (CVE-2015-6563)

- A privilege escalation vulnerability exists due to a use-after-free error in sshd that is triggered when handling a MONITOR_REQ_PAM_FREE_CTX request. A local attacker can exploit this to gain elevated privileges.

Note that this issue only affects Portable OpenSSH.

(CVE-2015-6564)

- A local command execution vulnerability exists in sshd due to setting insecure world-writable permissions for TTYs. A local attacker can exploit this, by injecting crafted terminal escape sequences, to execute commands for logged-in users. (CVE-2015-6565)

See Also

http://www.openssh.com/txt/release-7.0

Solution

Upgrade to OpenSSH 7.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.3465

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	75990
BID	76317
BID	76497
CVE	CVE-2015-5600
CVE	CVE-2015-6563
CVE	CVE-2015-6564
CVE	CVE-2015-6565
XREF	EDB-ID:41173

Plugin Information

Published: 2015/08/13, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 7.0
```

90023 - OpenSSH < 7.2p2 X11Forwarding xauth Command Injection

Synopsis

The SSH server running on the remote host is affected by a security bypass vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.2p2. It is, therefore, affected by a security bypass vulnerability due to improper sanitization of X11 authentication credentials. An authenticated, remote attacker can exploit this, via crafted credentials, to inject arbitrary xauth commands, resulting in gaining read and write access to arbitrary files, connecting to local ports, or performing further attacks on xauth itself. Note that exploiting this vulnerability requires X11Forwarding to have been enabled.

See Also

http://www.openssh.com/txt/release-7.2p2

http://www.openssh.com/txt/x11fwd.adv

Solution

Upgrade to OpenSSH version 7.2p2 / 7.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.8

EPSS Score

0.0121

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-3115
XREF	EDB-ID:39569

Plugin Information

Published: 2016/03/18, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 7.2p2 / 7.3
```

99359 - OpenSSH < 7.5

Synopsis

The SSH server running on the remote host is affected by an information disclosure vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.5. It is, therefore, affected by an information disclosure vulnerability :

- An unspecified timing flaw exists in the CBC padding oracle countermeasures, within the ssh and sshd functions, that allows an unauthenticated, remote attacker to disclose potentially sensitive information.

Note that the OpenSSH client disables CBC ciphers by default. However, sshd offers them as lowest-preference options, which will be removed by default in a future release.

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

See Also

http://www.openssh.com/txt/release-7.5

Solution

Upgrade to OpenSSH version 7.5 or later.

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

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

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)

Plugin Information

Published: 2017/04/13, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 7.5
```

103781 - OpenSSH < 7.6

Synopsis

The SSH server running on the remote host is affected by a file creation restriction bypass vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.6. It is, therefore, affected by a file creation restriction bypass vulnerability related to the 'process_open'

function in the file 'sftp-server.c' that allows authenticated users to create zero-length files regardless of configuration.

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

See Also

http://www.nessus.org/u?09ca048b

http://www.nessus.org/u?96a8ea52

http://www.openssh.com/txt/release-7.6

Solution

Upgrade to OpenSSH version 7.6 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 v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0036

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)

References

BID	101552
CVE	CVE-2017-15906

Plugin Information

Published: 2017/10/11, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 7.6
```

159490 - OpenSSH < 7.8

Synopsis

The SSH server running on the remote host is affected by a information disclosure vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.8. It is, therefore, affected by an information disclosure vulnerability in the auth2-gss.c, auth2-hostbased.c, and auth2-pubkey due to not delaying for an invalid authenticating user. An unauthenticated, remote attacker can exploit this, via a malformed packet, to potentially enumerate users.

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.openwall.com/lists/oss-security/2018/08/15/5

https://www.openssh.com/txt/release-7.8

Solution

Upgrade to OpenSSH version 7.8 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

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

VPR Score

4.9

EPSS Score

0.0331

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

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

References

CVE	CVE-2018-15473

Exploitable With

CANVAS (true)

Plugin Information

Published: 2022/04/04, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 7.8
```

159491 - OpenSSH < 8.0

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 8.0. It is, therefore, affected by the following vulnerabilities:

- A permission bypass vulnerability due to improper directory name validation. An unauthenticated, remote attacker can exploit this, with a specially crafted scp server, to change the permission of a directory on the client. (CVE-2018-20685)

- Multiple arbitrary file downloads due to improper validation of object name and stderr output. An unauthenticated remote attacker can exploit this, with a specially crafted scp server, to include additional hidden files in the transfer. (CVE-2019-6109, CVE-2019-6110)

- An arbitrary file write vulnerability due to improper object name validation. An unauthenticated, remote attacker can exploit this, with a specially crafted scp server, to overwrite arbitrary files in the client directory. (CVE-2019-6111)

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://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt

https://www.openssh.com/txt/release-8.0

Solution

Upgrade to OpenSSH version 8.0 or later.

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

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

VPR Score

6.1

EPSS Score

0.004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-20685
CVE	CVE-2019-6109
CVE	CVE-2019-6110
CVE	CVE-2019-6111

Plugin Information

Published: 2022/04/04, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 8.0
```

187201 - OpenSSH < 9.6 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

The version of OpenSSH installed on the remote host is prior to 9.6. It is, therefore, affected by multiple vulnerabilities as referenced in the release-9.6 advisory.

- ssh(1), sshd(8): implement protocol extensions to thwart the so-called Terrapin attack discovered by Fabian Bumer, Marcus Brinkmann and Jrg Schwenk. This attack allows a MITM to effect a limited break of the integrity of the early encrypted SSH transport protocol by sending extra messages prior to the commencement of encryption, and deleting an equal number of consecutive messages immediately after encryption starts. A peer SSH client/server would not be able to detect that messages were deleted. While cryptographically novel, the security impact of this attack is fortunately very limited as it only allows deletion of consecutive messages, and deleting most messages at this stage of the protocol prevents user user authentication from proceeding and results in a stuck connection. The most serious identified impact is that it lets a MITM to delete the SSH2_MSG_EXT_INFO message sent before authentication starts, allowing the attacker to disable a subset of the keystroke timing obfuscation features introduced in OpenSSH 9.5.

There is no other discernable impact to session secrecy or session integrity. OpenSSH 9.6 addresses this protocol weakness through a new strict KEX protocol extension that will be automatically enabled when both the client and server support it. This extension makes two changes to the SSH transport protocol to improve the integrity of the initial key exchange. Firstly, it requires endpoints to terminate the connection if any unnecessary or unexpected message is received during key exchange (including messages that were previously legal but not strictly required like SSH2_MSG_DEBUG). This removes most malleability from the early protocol. Secondly, it resets the Message Authentication Code counter at the conclusion of each key exchange, preventing previously inserted messages from being able to make persistent changes to the sequence number across completion of a key exchange. Either of these changes should be sufficient to thwart the Terrapin Attack. More details of these changes are in the PROTOCOL file in the OpenSSH source distribition. (CVE-2023-48795)

- ssh-agent(1): when adding PKCS#11-hosted private keys while specifying destination constraints, if the PKCS#11 token returned multiple keys then only the first key had the constraints applied. Use of regular private keys, FIDO tokens and unconstrained keys are unaffected. (CVE-2023-51384)

- ssh(1): if an invalid user or hostname that contained shell metacharacters was passed to ssh(1), and a ProxyCommand, LocalCommand directive or match exec predicate referenced the user or hostname via %u, %h or similar expansion token, then an attacker who could supply arbitrary user/hostnames to ssh(1) could potentially perform command injection depending on what quoting was present in the user-supplied ssh_config(5) directive. This situation could arise in the case of git submodules, where a repository could contain a submodule with shell characters in its user/hostname. Git does not ban shell metacharacters in user or host names when checking out repositories from untrusted sources. Although we believe it is the user's responsibility to ensure validity of arguments passed to ssh(1), especially across a security boundary such as the git example above, OpenSSH 9.6 now bans most shell metacharacters from user and hostnames supplied via the command-line. This countermeasure is not guaranteed to be effective in all situations, as it is infeasible for ssh(1) to universally filter shell metacharacters potentially relevant to user-supplied commands. User/hostnames provided via ssh_config(5) are not subject to these restrictions, allowing configurations that use strange names to continue to be used, under the assumption that the user knows what they are doing in their own configuration files. (CVE-2023-51385)

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.openssh.com/txt/release-9.6

Solution

Upgrade to OpenSSH version 9.6 or later.

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 v3.0 Temporal Score

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

VPR Score

6.1

EPSS Score

0.9548

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-48795
CVE	CVE-2023-51384
CVE	CVE-2023-51385
XREF	IAVA:2023-A-0701-S

Plugin Information

Published: 2023/12/22, Modified: 2024/07/05

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 9.6p1 / 9.6
```

67140 - OpenSSH LoginGraceTime / MaxStartups DoS

Synopsis

The remote SSH service is susceptible to a remote denial of service attack.

Description

According to its banner, a version of OpenSSH earlier than version 6.2 is listening on this port. The default configuration of OpenSSH installs before 6.2 could allow a remote attacker to bypass the LoginGraceTime and MaxStartups thresholds by periodically making a large number of new TCP connections and thereby prevent legitimate users from gaining access to the service.

Note that this plugin has not tried to exploit the issue or detect whether the remote service uses a vulnerable configuration. Instead, it has simply checked the version of OpenSSH running on the remote host.

See Also

https://www.openwall.com/lists/oss-security/2013/02/06/5

http://openssh.org/txt/release-6.2

https://tools.cisco.com/security/center/viewAlert.x?alertId=28883

Solution

Upgrade to OpenSSH 6.2 and review the associated server configuration settings.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.0787

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	58162
CVE	CVE-2010-5107

Plugin Information

Published: 2013/07/03, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 6.2
```

31737 - OpenSSH X11 Forwarding Session Hijacking

Synopsis

The remote SSH service is prone to an X11 session hijacking vulnerability.

Description

According to its banner, the version of SSH installed on the remote host is older than 5.0. Such versions may allow a local user to hijack X11 sessions because it improperly binds TCP ports on the local IPv6 interface if the corresponding ports on the IPv4 interface are in use.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011

https://www.openssh.com/txt/release-5.0

Solution

Upgrade to OpenSSH version 5.0 or later.

Risk Factor

Medium

VPR Score

6.0

EPSS Score

0.0099

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

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

References

BID	28444
CVE	CVE-2008-1483
CVE	CVE-2008-3234
XREF	Secunia:29522

XREF CWE:264

Plugin Information

Published: 2008/04/03, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 5.0
```

74326 - OpenSSL 'ChangeCipherSpec' MiTM Potential Vulnerability

Synopsis

The remote host is potentially affected by a vulnerability that could allow sensitive data to be decrypted.

Description

The OpenSSL service on the remote host is potentially vulnerable to a man-in-the-middle (MiTM) attack, based on its response to two consecutive 'ChangeCipherSpec' messages during the incorrect phase of an SSL/TLS handshake.

This flaw could allow a MiTM attacker to decrypt or forge SSL messages by telling the service to begin encrypted communications before key material has been exchanged, which causes predictable keys to be used to secure future traffic.

OpenSSL 1.0.1 is known to be exploitable. OpenSSL 0.9.8 and 1.0.0 are not known to be vulnerable; however, the OpenSSL team has advised that users of these older versions upgrade as a precaution. This plugin detects and reports all versions of OpenSSL that are potentially exploitable.

Note that Nessus has only tested for an SSL/TLS MiTM vulnerability (CVE-2014-0224). However, Nessus has inferred that the OpenSSL service on the remote host is also affected by six additional vulnerabilities that were disclosed in OpenSSL's June 5th, 2014 security advisory :

- An error exists in the 'ssl3_read_bytes' function that permits data to be injected into other sessions or allows denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2010-5298)

- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that allows nonce disclosure via the 'FLUSH+RELOAD' cache side-channel attack. (CVE-2014-0076)

- A buffer overflow error exists related to invalid DTLS fragment handling that permits the execution of arbitrary code or allows denial of service attacks.

Note that this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195)

- An error exists in the 'do_ssl3_write' function that permits a NULL pointer to be dereferenced, which could allow denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2014-0198)

- An error exists related to DTLS handshake handling that could allow denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client.

(CVE-2014-0221)

- An error exists in the 'dtls1_get_message_fragment'

function related to anonymous ECDH cipher suites. This could allow denial of service attacks. Note that this issue only affects OpenSSL TLS clients. (CVE-2014-3470)

OpenSSL did not release individual patches for these vulnerabilities, instead they were all patched under a single version release. Note that the service will remain vulnerable after patching until the service or host is restarted.

See Also

http://www.nessus.org/u?d5709faa

https://www.imperialviolet.org/2014/06/05/earlyccs.html

https://www.openssl.org/news/secadv/20140605.txt

Solution

OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Risk Factor

Medium

VPR Score

7.7

EPSS Score

0.9754

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)

References

BID	66363
BID	66801
BID	67193
BID	67898
BID	67899
BID	67900
BID	67901
CVE	CVE-2010-5298
CVE	CVE-2014-0076
CVE	CVE-2014-0195
CVE	CVE-2014-0198
CVE	CVE-2014-0221
CVE	CVE-2014-0224
CVE	CVE-2014-3470
XREF	CERT:978508

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/06/05, Modified: 2020/06/12

Plugin Output

tcp/25/smtp

```
The remote service accepted two consecutive ChangeCipherSpec messages at an incorrect point in the
handshake, without closing the connection or sending an SSL alert. This behavior indicates that the
service is vulnerable; however, this could also be the result of network interference.
```

74326 - OpenSSL 'ChangeCipherSpec' MiTM Potential Vulnerability

Synopsis

The remote host is potentially affected by a vulnerability that could allow sensitive data to be decrypted.

Description

The OpenSSL service on the remote host is potentially vulnerable to a man-in-the-middle (MiTM) attack, based on its response to two consecutive 'ChangeCipherSpec' messages during the incorrect phase of an SSL/TLS handshake.

This flaw could allow a MiTM attacker to decrypt or forge SSL messages by telling the service to begin encrypted communications before key material has been exchanged, which causes predictable keys to be used to secure future traffic.

OpenSSL 1.0.1 is known to be exploitable. OpenSSL 0.9.8 and 1.0.0 are not known to be vulnerable; however, the OpenSSL team has advised that users of these older versions upgrade as a precaution. This plugin detects and reports all versions of OpenSSL that are potentially exploitable.

Note that Nessus has only tested for an SSL/TLS MiTM vulnerability (CVE-2014-0224). However, Nessus has inferred that the OpenSSL service on the remote host is also affected by six additional vulnerabilities that were disclosed in OpenSSL's June 5th, 2014 security advisory :

- An error exists in the 'ssl3_read_bytes' function that permits data to be injected into other sessions or allows denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2010-5298)

- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that allows nonce disclosure via the 'FLUSH+RELOAD' cache side-channel attack. (CVE-2014-0076)

- A buffer overflow error exists related to invalid DTLS fragment handling that permits the execution of arbitrary code or allows denial of service attacks.

Note that this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195)

- An error exists in the 'do_ssl3_write' function that permits a NULL pointer to be dereferenced, which could allow denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2014-0198)

- An error exists related to DTLS handshake handling that could allow denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client.

(CVE-2014-0221)

- An error exists in the 'dtls1_get_message_fragment'

function related to anonymous ECDH cipher suites. This could allow denial of service attacks. Note that this issue only affects OpenSSL TLS clients. (CVE-2014-3470)

OpenSSL did not release individual patches for these vulnerabilities, instead they were all patched under a single version release. Note that the service will remain vulnerable after patching until the service or host is restarted.

See Also

http://www.nessus.org/u?d5709faa

https://www.imperialviolet.org/2014/06/05/earlyccs.html

https://www.openssl.org/news/secadv/20140605.txt

Solution

OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Risk Factor

Medium

VPR Score

7.7

EPSS Score

0.9754

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)

References

BID	66363
BID	66801
BID	67193
BID	67898
BID	67899
BID	67900
BID	67901
CVE	CVE-2010-5298
CVE	CVE-2014-0076
CVE	CVE-2014-0195
CVE	CVE-2014-0198
CVE	CVE-2014-0221
CVE	CVE-2014-0224
CVE	CVE-2014-3470
XREF	CERT:978508

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/06/05, Modified: 2020/06/12

Plugin Output

tcp/5432/postgresql

```
The remote service accepted an SSL ChangeCipherSpec message at an incorrect point in the handshake
leading to weak keys being used, and then attempted to decrypt an SSL record using those weak keys.
This plugin detects unpatched OpenSSL 1.0.1, 1.0.0, and 0.9.8 services. Only 1.0.1 has been shown
 to
be exploitable; however, OpenSSL 1.0.0 and 0.9.8 have received similar patches and users of these
versions have been advised to upgrade as a precaution.
```

51139 - PHP 5.2 < 5.2.15 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP 5.2 installed on the remote host is older than 5.2.15. Such versions may be affected by several security issues :

- A crash in the zip extract method.

- A possible double free exists in the imap extension.

(CVE-2010-4150)

- An unspecified flaw exists in 'open_basedir'. (CVE-2010-3436)

- A possible crash could occur in 'mssql_fetch_batch()'.

- A NULL pointer dereference exists in 'ZipArchive::getArchiveComment'. (CVE-2010-3709)

- A crash exists if anti-aliasing steps are invalid.

(Bug #53492)

- A crash exists in pdo_firebird getAttribute(). (Bug #53323)

- A user-after-free vulnerability in the Zend engine when a '__set()', '__get()', '__isset()' or '__unset()' method is called can allow for a denial of service attack. (Bug #52879 / CVE-2010-4697)

- A stack-based buffer overflow exists in the 'imagepstext()' function in the GD extension. (Bug #53492 / CVE-2010-4698)

- The extract function does not prevent use of the EXTR_OVERWRITE parameter to overwrite the GLOBALS superglobal array and the 'this' variable, which allows attackers to bypass intended access restrictions.

(CVE-2011-0752)

See Also

http://www.php.net/releases/5_2_15.php

http://www.php.net/ChangeLog-5.php#5.2.15

Solution

Upgrade to PHP version 5.2.15 or later.

Risk Factor

Medium

VPR Score

5.8

EPSS Score

0.0237

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	44718
BID	44723
BID	45335
BID	45952
BID	46448
CVE	CVE-2010-3436
CVE	CVE-2010-3709
CVE	CVE-2010-4150
CVE	CVE-2010-4697
CVE	CVE-2010-4698
CVE	CVE-2011-0752

Plugin Information

Published: 2010/12/13, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.15
```

51439 - PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS

Synopsis

The remote web server uses a version of PHP that is affected by a denial of service vulnerability.

Description

According to its banner, the version of PHP 5.x installed on the remote host is older than 5.2.17 or 5.3.5.

Such versions may experience a crash while performing string to double conversion for certain numeric values. Only x86 32-bit PHP processes are known to be affected by this issue regardless of whether the system running PHP is 32-bit or 64-bit.

See Also

https://bugs.php.net/bug.php?id=53632

http://www.php.net/distributions/test_bug53632.txt

http://www.php.net/releases/5_2_17.php

http://www.php.net/releases/5_3_5.php

Solution

Upgrade to PHP 5.2.17/5.3.5 or later.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.0163

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

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

References

BID	45668

CVE CVE-2010-4645

Plugin Information

Published: 2011/01/07, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.17/5.3.5
```

58681 - PHP 5.2.x filter_globals Subsequence Request Parsing Remote Code Execution

Synopsis

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

Description

According to its banner, the version of PHP installed on the remote host is in the 5.2 release branch. As such, it reportedly may be affected by a remote code execution vulnerability.

An error in the file 'ext/filter/filter.c' does not properly clear the 'filter_globals' struct if PHP encounters issues during its start up process. This struct then contains stale values and can allow an attacker to use a specially crafted request to crash PHP, obtain sensitive information or possibly execute arbitrary code.

Note that this issue reportedly only affects PHP when running as an Apache module and not in other configurations such as CGI, nor when used with other web servers such as IIS.

See Also

http://www.php.net/ChangeLog-5.php#5.3.0

https://seclists.org/bugtraq/2012/Feb/93

https://bugs.php.net/bug.php?id=47930

http://svn.php.net/viewvc?view=revision&revision=279522

Solution

Upgrade to PHP version 5.3.0 or later.

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 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	52065

Plugin Information

Published: 2012/04/11, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.3.0
```

39480 - PHP < 5.2.10 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 older than 5.2.10. Such versions are reportedly affected by multiple vulnerabilities :

- Sufficient checks are not performed on fields reserved for offsets in function 'exif_read_data()'. Successful exploitation of this issue could result in a denial of service condition. (bug 48378)

- Provided 'safe_mode_exec_dir' is not set (not set by default), it may be possible to bypass 'safe_mode' restrictions by preceding a backslash in functions such as 'exec()', 'system()', 'shell_exec()', 'passthru()' and 'popen()' on a system running PHP on Windows. (bug 45997)

See Also

https://bugs.php.net/bug.php?id=45997

https://bugs.php.net/bug.php?id=48378

http://www.php.net/releases/5_2_10.php

http://www.php.net/ChangeLog-5.php#5.2.10

Solution

Upgrade to PHP version 5.2.10 or later.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.0177

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	35435
BID	35440
CVE	CVE-2009-2687
XREF	SECUNIA:35441
XREF	CWE:20

Plugin Information

Published: 2009/06/22, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.10
```

43351 - PHP < 5.2.12 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.12. Such versions may be affected by several security issues :

- It is possible to bypass the 'safe_mode' configuration setting using 'tempnam()'. (CVE-2009-3557)

- It is possible to bypass the 'open_basedir' configuration setting using 'posix_mkfifo()'. (CVE-2009-3558)

- Provided file uploading is enabled (it is by default), an attacker can upload files using a POST request with 'multipart/form-data' content even if the target script doesn't actually support file uploads per se. By supplying a large number (15,000+) of files, an attacker could cause the web server to stop responding while it processes the file list. (CVE-2009-4017)

- Missing protection for '$_SESSION' from interrupt corruption and improved 'session.save_path' check. (CVE-2009-4143)

- Insufficient input string validation in the 'htmlspecialchars()' function. (CVE-2009-4142)

See Also

http://www.nessus.org/u?57f2d08f

http://www.php.net/releases/5_2_12.php

http://www.php.net/ChangeLog-5.php#5.2.12

Solution

Upgrade to PHP version 5.2.12 or later.

Risk Factor

Medium

VPR Score

6.7

EPSS Score

0.0905

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	37389
BID	37390
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-4017
CVE	CVE-2009-4142
CVE	CVE-2009-4143
XREF	SECUNIA:37821
XREF	CWE:79
XREF	CWE:264

Plugin Information

Published: 2009/12/18, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.12
```

28181 - PHP < 5.2.5 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.5. Such versions may be affected by various issues, including but not limited to several buffer overflows.

See Also

http://www.php.net/releases/5_2_5.php

Solution

Upgrade to PHP version 5.2.5 or later.

Risk Factor

Medium

VPR Score

6.7

EPSS Score

0.0565

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	26403
BID	69246
CVE	CVE-2007-3996
CVE	CVE-2007-4782
CVE	CVE-2007-4783
CVE	CVE-2007-4784

CVE	CVE-2007-4825
CVE	CVE-2007-4840
CVE	CVE-2007-4887
CVE	CVE-2007-4889
CVE	CVE-2007-5447
CVE	CVE-2007-5653
CVE	CVE-2007-5898
CVE	CVE-2007-5899
CVE	CVE-2007-5900
CVE	CVE-2008-2107
CVE	CVE-2008-2108
CVE	CVE-2008-4107
XREF	CWE:20
XREF	CWE:22
XREF	CWE:78
XREF	CWE:94
XREF	CWE:189
XREF	CWE:200
XREF	CWE:264

Plugin Information

Published: 2007/11/12, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.5
```

35750 - PHP < 5.2.9 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such versions may be affected by several security issues :

- Background color is not correctly validated with a non true color image in function 'imagerotate()'. (CVE-2008-5498)

- A denial of service condition can be triggered by trying to extract zip files that contain files with relative paths in file or directory names.

- Function 'explode()' is affected by an unspecified vulnerability.

- It may be possible to trigger a segfault by passing a specially crafted string to function 'json_decode()'.

- Function 'xml_error_string()' is affected by a flaw which results in messages being off by one.

See Also

http://news.php.net/php.internals/42762

http://www.php.net/releases/5_2_9.php

http://www.php.net/ChangeLog-5.php#5.2.9

Solution

Upgrade to PHP version 5.2.9 or later.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.0973

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

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

References

BID	33002
BID	33927
CVE	CVE-2008-5498
CVE	CVE-2009-1271
CVE	CVE-2009-1272
XREF	SECUNIA:34081
XREF	CWE:20
XREF	CWE:200

Plugin Information

Published: 2009/02/27, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.2.9
```

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

EPSS Score

0.0257

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: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.3.11
```

44921 - PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.2 / 5.2.13. Such versions may be affected by several security issues :

- Directory paths not ending with '/' may not be correctly validated inside 'tempnam()' in 'safe_mode' configuration.

- It may be possible to bypass the 'open_basedir'/ 'safe_mode' configuration restrictions due to an error in session extensions.

- An unspecified vulnerability affects the LCG entropy.

See Also

http://securityreason.com/achievement_securityalert/82

http://securityreason.com/securityalert/7008

https://seclists.org/fulldisclosure/2010/Feb/208

http://www.php.net/releases/5_3_2.php

http://www.php.net/ChangeLog-5.php#5.3.2

http://www.php.net/releases/5_2_13.php

http://www.php.net/ChangeLog-5.php#5.2.13

Solution

Upgrade to PHP version 5.3.2 / 5.2.13 or later.

Risk Factor

Medium

VPR Score

5.3

EPSS Score

0.0176

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	38182
BID	38430
BID	38431
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
XREF	SECUNIA:38708

Plugin Information

Published: 2010/02/26, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source     : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version  : 5.2.4-2ubuntu5.10
  Fixed version      : 5.3.2 / 5.2.13
```

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: 2024/11/22

Plugin Output

tcp/80/www

```
 URL              : http://Epic-Metasploitable.epicode/ (5.2.4-2ubuntu5.10 under X-Powered-By:
PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/phpinfo.php)
 Installed version : 5.2.4-2ubuntu5.10
 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

EPSS Score

0.0029

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: 2024/11/22

Plugin Output

tcp/80/www

```
  Version source    : X-Powered-By: PHP/5.2.4-2ubuntu5.10, http://Epic-Metasploitable.epicode/
phpinfo.php
  Installed version : 5.2.4-2ubuntu5.10
  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/80/www

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

  http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/DBMS.php/?=PHPB8B5F2A0-3C92-11d3-
A3A9-4C7B08C10000
```

63348 - PostgreSQL 7.4 < 7.4.27 / 8.0 < 8.0.23 / 8.1 < 8.1.19 / 8.2 < 8.2.15 / 8.3 < 8.3.9 / 8.4 < 8.4.2 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of PostgreSQL installed on the remote host is 7.4 prior to 7.4.27, 8.0 prior to 8.0.23, 8.1 prior to 8.1.19, 8.2 prior to 8.2.15, 8.3 prior to 8.3.9 or 8.4 prior to 8.4.2. As such, it is potentially affected by multiple vulnerabilities :

- NULL bytes in SSL Certificates can be used to falsify client or server authentication. (CVE-2009-4034)

- Privilege escalation is possible via changing session state in an index function. (CVE-2009-4136)

See Also

https://www.postgresql.org/about/news/1170/

https://www.postgresql.org/docs/7.4/release-7-4-27.html

https://www.postgresql.org/docs/8.0/release-8-0-23.html

https://www.postgresql.org/docs/8.1/release-8-1-19.html

https://www.postgresql.org/docs/8.2/release-8-2-15.html

https://www.postgresql.org/docs/8.3/release-8-3-9.html

https://www.postgresql.org/docs/8.4/release-8-4-2.html

Solution

Upgrade to PostgreSQL 7.4.27 / 8.0.23 / 8.1.19 / 8.2.15 / 8.3.9 / 8.4.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0384

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	37333
BID	37334
CVE	CVE-2009-4034
CVE	CVE-2009-4136
XREF	CWE:310

Plugin Information

Published: 2012/12/28, Modified: 2024/10/23

Plugin Output

tcp/5432/postgresql

```
Version source    : Fauth.c.L1003.Rauth_failed
Installed version : 8.3.8
Fixed version     : 7.4.27 / 8.0.23 / 8.1.19 / 8.2.15 / 8.3.9 / 8.4.2
```

63350 - PostgreSQL 7.4 < 7.4.30 / 8.0 < 8.0.26 / 8.1 < 8.1.22 / 8.2 < 8.2.18 / 8.3 < 8.3.12 / 8.4 < 8.4.5 / 9.0 < 9.0.1

Synopsis

The remote database server is affected by a privilege escalation vulnerability.

Description

The version of PostgreSQL installed on the remote host is 7.4 prior to 7.4.30, 8.0 prior to 8.0.26, 8.1 prior to 8.1.22, 8.2 prior to 8.2.18, 8.3 prior to 8.3.12, 8.4 prior to 8.4.5, or 9.0 prior to 9.0.1. It therefore is potentially affected by a privilege escalation vulnerability.

A remote, authenticated attacker could elevate privileges via specially crafted code in a SECURITY DEFINER function.

See Also

https://www.postgresql.org/about/news/1244/

https://www.postgresql.org/docs/7.4/release.html#RELEASE-7-4-30

https://www.postgresql.org/docs/8.0/release.html#RELEASE-8-0-26

https://www.postgresql.org/docs/8.1/release-8-1-22.html

https://www.postgresql.org/docs/8.2/release-8-2-18.html

https://www.postgresql.org/docs/8.3/release-8-3-12.html

http://www.postgresql.org/docs/8.4/static/release-8-4-5.html

https://www.postgresql.org/docs/9.0/release.html#RELEASE-9-0-1

Solution

Upgrade to PostgreSQL 7.4.30 / 8.0.26 / 8.1.22 / 8.2.18 / 8.3.12 / 8.4.5 / 9.0.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.4

EPSS Score

0.0353

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	43747
CVE	CVE-2010-3433

Plugin Information

Published: 2012/12/28, Modified: 2024/10/23

Plugin Output

tcp/5432/postgresql

```
Version source    : Fauth.c.L1003.Rauth_failed
Installed version : 8.3.8
Fixed version     : 7.4.30 / 8.0.26 / 8.1.22 / 8.2.18 / 8.3.12 / 8.4.5 / 9.0.1
```

63351 - PostgreSQL 8.2 < 8.2.20 / 8.3 < 8.3.14 / 8.4 < 8.4.7 / 9.0 < 9.0.3 Buffer Overflow Vulnerability

Synopsis

The remote database server is affected by a buffer overflow vulnerability.

Description

The version of PostgreSQL installed on the remote host is 8.2.x prior to 8.2.20, 8.3.x prior to 8.3.14, 8.4.x prior to 8.4.7, or 9.0.x prior to 9.0.3. It therefore is potentially affected by a buffer overflow vulnerability.

By calling functions from the intarray optional module with certain parameters, a remote, authenticated attacker could execute arbitrary code on the remote host subject to the privileges of the user running the affected application.

See Also

https://www.postgresql.org/about/news/1289/

https://www.postgresql.org/docs/8.2/release-8-2-20.html

https://www.postgresql.org/docs/8.3/release-8-3-14.html

http://www.postgresql.org/docs/8.4/static/release-8-4-7.html

https://www.postgresql.org/docs/9.0/release-9-0-3.html

Solution

Upgrade to PostgreSQL 8.2.20 / 8.3.14 / 8.4.7 / 9.0.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.5

EPSS Score

0.0183

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	46084
CVE	CVE-2010-4015

Plugin Information

Published: 2012/12/28, Modified: 2024/10/23

Plugin Output

tcp/5432/postgresql

```
Version source    : Fauth.c.L1003.Rauth_failed
Installed version : 8.3.8
Fixed version     : 8.2.20 / 8.3.14 / 8.4.7 / 9.0.3
```

63354 - PostgreSQL 8.3 < 8.3.20 / 8.4 < 8.4.13 / 9.0 < 9.0.9 / 9.1 < 9.1.5 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of PostgreSQL installed on the remote host is 8.3.x prior to 8.3.20, 8.4.x prior to 8.4.13, 9.0.x prior to 9.0.9, or 9.1.x prior to 9.1.5. It therefore is potentially affected by multiple vulnerabilities :

- A flaw in contrib/xml2's xslt_process can be used to read and write arbitrary files. (CVE-2012-3488)

- An xml_parse() DTD validation flaw can be used to read arbitrary files. (CVE-2012-3489)

See Also

http://www.postgresql.org/about/news/1407/

https://www.postgresql.org/docs/8.3/release-8-3-20.html

http://www.postgresql.org/docs/8.4/static/release-8-4-13.html

https://www.postgresql.org/docs/9.0/release-9-0-9.html

http://www.postgresql.org/docs/9.1/static/release-9-1-5.html

Solution

Upgrade to PostgreSQL 8.3.20 / 8.4.13 / 9.0.9 / 9.1.5 or later.

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 v3.0 Temporal Score

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

VPR Score

6.5

EPSS Score

0.0021

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	55072
BID	55074
CVE	CVE-2012-3488
CVE	CVE-2012-3489

Plugin Information

Published: 2012/12/28, Modified: 2024/10/23

Plugin Output

tcp/5432/postgresql

```
Version source    : Fauth.c.L1003.Rauth_failed
Installed version : 8.3.8
Fixed version     : 8.3.20 / 8.4.13 / 9.0.9 / 9.1.5
```

64669 - PostgreSQL 8.3 < 8.3.23 / 8.4 < 8.4.16 / 9.0 < 9.0.12 / 9.1 < 9.1.8 / 9.2 < 9.2.3 Denial of Service

Synopsis

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

Description

The version of PostgreSQL installed on the remote host is 8.3.x prior to 8.3.23, 8.4.x prior to 8.4.16, 9.0.x prior to 9.0.12, 9.1.x prior to 9.1.8 or 9.2 prior to 9.2.3. It is, therefore, potentially affected by a denial of service vulnerability due to a flaw in the enum_recv() function of 'backend/utils/adt/enum.c'. By exploiting this flaw, a remote attacker could crash the affected application.

See Also

https://www.postgresql.org/about/news/1446/

https://www.postgresql.org/docs/8.3/release-8-3-23.html

https://www.postgresql.org/docs/8.4/release-8-4-16.html

https://www.postgresql.org/docs/9.0/release-9-0-12.html

http://www.postgresql.org/docs/9.1/static/release-9-1-8.html

http://www.postgresql.org/docs/9.2/static/release-9-2-3.html

Solution

Upgrade to PostgreSQL 8.3.23 / 8.4.16 / 9.0.12 / 9.1.8 / 9.2.3 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:N/A:L)

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0172

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	57844
CVE	CVE-2013-0255

Plugin Information

Published: 2013/02/18, Modified: 2024/10/23

Plugin Output

tcp/5432/postgresql

```
Version source    : Fauth.c.L1003.Rauth_failed
Installed version : 8.3.8
Fixed version     : 8.3.23 / 8.4.16 / 9.0.12 / 9.1.8 / 9.2.3
```

106752 - ProFTPD < 1.3.2b / 1.3.3x < 1.3.3rc2 client-hostname restriction bypass

Synopsis

The remote FTP server is affected by a Denial of Service vulnerability.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

According to its banner, the version of ProFTPD installed on the remote host is 1.3.2x prior to 1.3.2b or 1.3.3x prior to 1.3.3rc2 and is affected by a mitigation bypass vulnerability when the dNSNameRequired TLS option is enabled.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=3275

Solution

Upgrade to ProFTPD version 1.3.2b / 1.3.3rc2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.5

EPSS Score

0.005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	36804
CVE	CVE-2009-3639
XREF	CWE:310

Plugin Information

Published: 2018/02/12, Modified: 2019/11/08

Plugin Output

tcp/2121/ftp

```
  Version source    : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
500 GET not understood
  Installed version : 1.3.1
  Fixed version     : 1.3.2b / 1.3.3rc2
```

106751 - ProFTPD < 1.3.2rc3 ABOR Denial of Service

Synopsis

The remote FTP server is affected by a Denial of Service vulnerability.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

According to its banner, the version of ProFTPD installed on the remote host is earlier than 1.3.2rc3 and is affected by a Denial of Service vulnerability via an ABOR command during a data transfer.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=3131

https://www.debian.org/security/2011/dsa-2191

Solution

Upgrade to ProFTPD version 1.3.2rc3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0015

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	84378
CVE	CVE-2008-7265

Plugin Information

Published: 2018/02/12, Modified: 2019/11/08

Plugin Output

tcp/2121/ftp

```
  Version source    : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
500 GET not understood
  Installed version : 1.3.1
  Fixed version     : 1.3.2rc3
```

51366 - ProFTPD < 1.3.3d 'mod_sql' Buffer Overflow

Synopsis

The remote FTP server is affected by a heap-based buffer overflow vulnerability.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

According to its banner, the version of ProFTPD installed on the remote host is earlier than 1.3.3d. Such versions are reportedly affected by a heap-based buffer overflow vulnerability in the function 'sql_prepare_where()' in the file 'contrib/mod_sql.c'. An unauthenticated, remote attacker may be able to exploit this in combination with an earlier SQL injection vulnerability (CVE-2009-0542) to execute arbitrary code with root privileges.

Note that Nessus did not actually test for the flaw but instead has relied on the version in ProFTPD's banner.

See Also

http://phrack.org/issues/67/7.html#article

http://bugs.proftpd.org/show_bug.cgi?id=3536

http://www.nessus.org/u?43c39fae

Solution

Upgrade to ProFTPD version 1.3.3d or later.

Risk Factor

Medium

VPR Score

6.7

EPSS Score

0.1596

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	44933
CVE	CVE-2010-4652

Plugin Information

Published: 2010/12/23, Modified: 2020/03/27

Plugin Output

tcp/2121/ftp

```
  Version source    : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
500 GET not understood
  Installed version : 1.3.1
  Fixed version     : 1.3.3d
```

106753 - ProFTPD < 1.3.4rc2 client-hostname restriction bypass

Synopsis

The remote FTP server is affected by a Denial of Service vulnerability.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

According to its banner, the version of ProFTPD installed on the remote host is earlier than 1.3.4rc2 and is affected by a Denial of Service vulnerability in the mod_sftp module.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=3586

Solution

Upgrade to ProFTPD version 1.3.4rc2 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:N/A:L)

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.0802

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

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

References

BID	46183
CVE	CVE-2011-1137

Plugin Information

Published: 2018/02/12, Modified: 2019/11/08

Plugin Output

tcp/2121/ftp

```
  Version source    : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
500 GET not understood
  Installed version : 1.3.1
  Fixed version     : 1.3.4rc2
```

106756 - ProFTPD < 1.3.5e / 1.3.6x < 1.3.6rc5 AllowChrootSymlinks bypass

Synopsis

The remote FTP server is affected by a mitigation bypass vulnerability.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

According to its banner, the version of ProFTPD installed on the remote host is prior to 1.3.5e or 1.3.6x prior to 1.3.6rc5 and is affected by an issue where an attacker who is not granted full filesystem access may reconfigure the home directory of an FTP user.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=4295

Solution

Upgrade to ProFTPD version 1.3.5e / 1.3.6rc5 or later.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	97409
CVE	CVE-2017-7418

Plugin Information

Published: 2018/02/12, Modified: 2019/11/08

Plugin Output

tcp/2121/ftp

```
  Version source    : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
500 GET not understood
  Installed version : 1.3.1
  Fixed version     : 1.3.5e / 1.3.6rc5
```

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

52611 - SMTP Service STARTTLS Plaintext Command Injection

Synopsis

The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

Description

The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.

Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

See Also

https://tools.ietf.org/html/rfc2487

https://www.securityfocus.com/archive/1/516901/30/0/threaded

Solution

Contact the vendor to see if an update is available.

Risk Factor

Medium

VPR Score

7.3

EPSS Score

0.0135

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	46767

CVE	CVE-2011-0411
CVE	CVE-2011-1430
CVE	CVE-2011-1431
CVE	CVE-2011-1432
CVE	CVE-2011-1506
CVE	CVE-2011-2165
XREF	CERT:555316

Plugin Information

Published: 2011/03/10, Modified: 2019/03/06

Plugin Output

tcp/25/smtp

```
Nessus sent the following two commands in a single packet :

  STARTTLS\r\nRSET\r\n

And the server sent the following two responses :

  220 2.0.0 Ready to start TLS
  250 2.0.0 Ok
```

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

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: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

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/25/smtp

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

|-Subject   : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Not After : Apr 16 14:07:45 2010 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=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

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/5432/postgresql

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

|-Subject   : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Not After : Apr 16 14:07:45 2010 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=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

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/25/smtp

```
The SSL certificate has already expired :

  Subject          : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Issuer           : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Not valid before : Mar 17 14:07:45 2010 GMT
  Not valid after  : Apr 16 14:07:45 2010 GMT
```

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/5432/postgresql

```
The SSL certificate has already expired :

  Subject          : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Issuer           : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Not valid before : Mar 17 14:07:45 2010 GMT
  Not valid after  : Apr 16 14:07:45 2010 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/25/smtp

```
The identities known by Nessus are :

  192.168.51.101
  Epic-Metasploitable.epicode

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

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/5432/postgresql

```
The identities known by Nessus are :

  192.168.51.101
  Epic-Metasploitable.epicode

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

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/25/smtp

```
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=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

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/5432/postgresql

```
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=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

58751 - SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)

Synopsis

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

Description

A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This plugin tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite and then solicits return data.

If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL \SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not be, depending on whether or not a countermeasure has been enabled.

Note that this plugin detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack, because the attack exploits the vulnerability at the client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

See Also

https://www.openssl.org/~bodo/tls-cbc.txt

https://www.imperialviolet.org/2011/09/23/chromeandbeast.html

https://vnhacker.blogspot.com/2011/09/beast.html

http://www.nessus.org/u?649b81c1

http://www.nessus.org/u?84775fd6

https://blogs.msdn.microsoft.com/kaushal/2012/01/20/fixing-the-beast/

Solution

Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported.

Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for 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:L/I:N/A:N)

VPR Score

2.9

EPSS Score

0.0143

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

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

STIG Severity

I

References

BID	49778
CVE	CVE-2011-3389
XREF	CERT:864643
XREF	MSFT:MS12-006
XREF	IAVB:2012-B-0006
XREF	CEA-ID:CEA-2019-0547

Plugin Information

Published: 2012/04/16, Modified: 2022/12/05

Plugin Output

tcp/25/smtp

```
Negotiated cipher suite: AES256-SHA|TLSv1|RSA|RSA|AES-CBC(256)|SHA1
```

82580 - Samba 3.0.0 'SamrChangePassword' RCE

Synopsis

The file and print server running on the remote host is affected by a remote code execution vulnerability.

Description

The version of Samba running on the remote host is affected by a remote code execution vulnerability due to improper validation of user-supplied input when passing RPC messages from external scripts to a shell. A remote, authenticated attacker can exploit this via the use of shell metacharacters during login negotiations when the 'username map script' option is enabled, or during the invocation of other printer and file management MS-RPC calls.

See Also

https://www.samba.org/samba/security/CVE-2007-2447.html

Solution

Upgrade to version 3.0.25 or later

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.9

EPSS Score

0.9359

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	23972
CVE	CVE-2007-2447
XREF	CERT:268336

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2015/04/06, Modified: 2020/03/09

Plugin Output

tcp/445/cifs

```
Nessus was able to run the following commands :
  sleep 3 (server's response was delayed by 3 seconds)
  sleep 9 (server's response was delayed by 9 seconds)
  sleep 15 (server's response was delayed by 15 seconds)
```

52503 - Samba 3.x < 3.3.15 / 3.4.12 / 3.5.7 'FD_SET' Memory Corruption

Synopsis

The remote Samba server is affected by a memory corruption vulnerability.

Description

According to its banner, the version of Samba 3.x running on the remote host is earlier than 3.3.15 / 3.4.12 / 3.5.7. An error exists in the range checks on file descriptors in the 'FD_SET' macro that allows stack corruption. This corruption can cause Samba to crash or to continually try selecting on an improper descriptor set.

An attacker who is able to get a connection to a file share, either authenticated or via a guest connection, can leverage this issue to launch a denial of service attack against the affected smbd service.

Note the possibility of arbitrary code execution exists with this type of vulnerability but has not been confirmed.

Also note that Nessus has not actually tried to exploit this issue or otherwise determine if one of the patches has been applied.

See Also

https://bugzilla.samba.org/show_bug.cgi?id=7949

http://www.samba.org/samba/security/CVE-2011-0719.html

https://www.samba.org/samba/history/samba-3.3.15.html

https://www.samba.org/samba/history/samba-3.4.12.html

https://www.samba.org/samba/history/samba-3.5.7.html

Solution

Either apply one of the patches referenced in the project's advisory or upgrade to 3.3.15 / 3.4.12 / 3.5.7 or later.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.0324

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	46597
CVE	CVE-2011-0719
XREF	Secunia:43512

Plugin Information

Published: 2011/03/02, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Installed version  : 3.0.20-Debian
Fixed version      : 3.3.15 / 3.4.12 / 3.5.7
```

55733 - Samba 3.x < 3.3.16 / 3.4.14 / 3.5.10 Multiple Vulnerabilities

Synopsis

The remote Samba server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Samba 3.x running on the remote host is earlier than 3.3.16 / 3.4.14 / 3.5.10. As such, it is potentially affected by several vulnerabilities in the Samba Web Administration Tool (SWAT) :

- A cross-site scripting vulnerability exists because of a failure to sanitize input to the username parameter of the 'passwd' program. (Issue #8289)

- A cross-site request forgery (CSRF) vulnerability can allow SWAT to be manipulated when a user who is logged in as root is tricked into clicking specially crafted URLs sent by an attacker. (Issue #8290)

Note that these issues are only exploitable when SWAT it enabled, and it is not enabled by default.

Also note that Nessus has relied only on the self-reported version number and has not actually determined whether SWAT is enabled, tried to exploit these issues, or determine if the associated patches have been applied.

See Also

https://bugzilla.samba.org/show_bug.cgi?id=8289

https://bugzilla.samba.org/show_bug.cgi?id=8290

https://www.samba.org/samba/security/CVE-2011-2522

https://www.samba.org/samba/security/CVE-2011-2694

https://www.samba.org/samba/history/samba-3.3.16.html

https://www.samba.org/samba/history/samba-3.4.14.html

https://www.samba.org/samba/history/samba-3.5.10.html

Solution

Either apply one of the patches referenced in the project's advisory or upgrade to 3.3.16 / 3.4.14 / 3.5.10 or later.

Risk Factor

Medium

VPR Score

6.7

EPSS Score

0.0343

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	48899
BID	48901
CVE	CVE-2011-2522
CVE	CVE-2011-2694
XREF	EDB-ID:17577
XREF	Secunia:45393

Plugin Information

Published: 2011/07/29, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Installed version  : 3.0.20-Debian
Fixed version      : 3.3.16 / 3.4.14 / 3.5.10
```

69276 - Samba 3.x < 3.5.22 / 3.6.x < 3.6.17 / 4.0.x < 4.0.8 read_nttrans_ea_lis DoS

Synopsis

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

Description

According to its banner, the version of Samba running on the remote host is 3.x prior to 3.5.22, 3.6.x prior to 3.6.17 or 4.0.x prior to 4.0.8. It is, therefore, potentially affected by a denial of service vulnerability.

An integer overflow error exists in the function 'read_nttrans_ea_lis'

in the file 'nttrans.c' that could allow denial of service attacks to be carried out via specially crafted network traffic.

Note if 'guest' connections are allowed, this issue can be exploited by a remote, unauthenticated attacker.

Further note that Nessus has relied only on the self-reported version number and has not actually tried to exploit this issue or determine if the associated patch has been applied.

See Also

https://www.samba.org/samba/security/CVE-2013-4124.html

https://www.samba.org/samba/history/samba-3.5.22.html

https://www.samba.org/samba/history/samba-3.6.17.html

https://www.samba.org/samba/history/samba-4.0.8.html

http://www.nessus.org/u?a31cffce

Solution

Either install the patch referenced in the project's advisory, or upgrade to version 3.5.22 / 3.6.17 / 4.0.8 or later.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.9683

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

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

References

BID	61597
CVE	CVE-2013-4124
XREF	EDB-ID:27778

Plugin Information

Published: 2013/08/08, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Installed version : 3.0.20-Debian
Fixed version     : 3.5.22 / 3.6.17 / 4.0.8
```

41970 - Samba < 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 Multiple Vulnerabilities

Synopsis

The remote Samba server may be affected by multiple vulnerabilities.

Description

According to its banner, the version of Samba server on the remote host is earlier than 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2. Such versions are potentially affected by multiple issues :

- If a user in '/etc/passwd' is misconfigured to have an empty home directory, then connecting to the home share of this user will use the root of the file system as the home directory. (CVE-2009-2813)

- Specially crafted SMB requests on authenticated SMB connections can send smbd into a 100% loop, causing a denial of service. (CVE-2009-2906)

- When 'mount.cifs' is installed as a setuid program, a user can pass it a credential or password path to which he or she does not have access and then use the '--verbose' option to view the first line of that file. (CVE-2009-2948)

See Also

https://www.samba.org/samba/security/CVE-2009-2906.html

https://www.samba.org/samba/security/CVE-2009-2948.html

https://www.samba.org/samba/security/CVE-2009-2813.html

Solution

Upgrade to Samba 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 or later.

Risk Factor

Medium

VPR Score

6.6

EPSS Score

0.016

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	36572
BID	36573
CVE	CVE-2009-2813
CVE	CVE-2009-2906
CVE	CVE-2009-2948
XREF	CWE:264

Plugin Information

Published: 2009/10/02, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
The remote Samba server appears to be :

  Samba 3.0.20-Debian
```

64459 - Samba < 3.5.21 / 3.6.12 / 4.0.2 SWAT Multiple Vulnerabilities

Synopsis

The remote Samba server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Samba running on the remote host is 3.5.x prior to 3.5.21, 3.6.x prior to 3.6.12, or 4.x prior to 4.0.1. It is, therefore, affected by the following vulnerabilities :

- An unspecified flaw exists in the Samba Web Administration Tool (SWAT) that allows a remote attacker to conduct clickjacking attacks via a FRAME or IFRAME element. (CVE-2013-0213)

- A cross-site request forgery vulnerability exists due to a failure to require multiple steps or explicit confirmation for sensitive transactions in the Samba Web Administration Tool (SWAT). A remote attacker can exploit this, by convincing a user to follow a crafted URL, to cause the user to perform unintended actions.

(CVE-2013-0213)

Note that these vulnerabilities are only exploitable when SWAT is enabled, and it is not enabled by default. Additionally, 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.samba.org/samba/security/CVE-2013-0213.html

https://www.samba.org/samba/security/CVE-2013-0214.html

https://www.samba.org/samba/history/samba-4.0.2.html

Solution

Upgrade to Samba version 3.5.21 / 3.6.12 / 4.0.2 or later.

Alternatively, install the patch referenced in the vendor advisory.

Risk Factor

Medium

VPR Score

5.9

EPSS Score

0.0425

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	57631
CVE	CVE-2013-0213
CVE	CVE-2013-0214

Plugin Information

Published: 2013/02/04, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Installed version  : 3.0.20-Debian
Fixed version      : 3.5.21 / 3.6.12 / 4.0.2
```

183023 - Samba < 4.17.12 / 4.18.x < 4.18.8 / 4.19.x < 4.19.1 Incorrect Permissions Handling

Synopsis

The remote Samba server is potentially affected by a vulnerability.

Description

The version of Samba running on the remote host is potentially affected by a vulnerability. The SMB protocol allows opening files where the client requests read-only access, but then implicitly truncating the opened file if the client specifies a separate OVERWRITE create disposition. This operation requires write access to the file, and in the default Samba configuration the operating system kernel will deny access to open a read-only file for read/write (which the truncate operation requires). However, when Samba has been configured to ignore kernel file system permissions, Samba will truncate a file when the underlying operating system kernel would deny the operation.

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.samba.org/samba/security/CVE-2023-4091.html

https://www.samba.org/samba/history/security.html

Solution

Upgrade to Samba version 4.17.12, 4.18.8, or 4.19.1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0015

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-4091
XREF	IAVA:2023-A-0535

Plugin Information

Published: 2023/10/13, Modified: 2023/11/14

Plugin Output

tcp/445/cifs

```
Installed version : 3.0.20-Debian
Fixed version     : 4.17.12
```

121041 - Sensitive File Disclosure

Synopsis

The web application hosts static files that may be sensitive in nature.

Description

The remote web application hosts documents or office files that may contain sensitive information.

Solution

Static files that are not necessary should be removed from the web root. If documents are required to be in the web root, and are sensitive in nature, they should require authentication.

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: 2019/01/09, Modified: 2025/01/22

Plugin Output

tcp/80/www

```
The following URLs are potentially sensitive documents :

  /mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
  /tomcat-docs/architecture/startup/serverStartup.pdf
  /tomcat-docs/architecture/requestProcess/requestProcess.pdf
```

20068 - TWiki %INCLUDE Parameter Arbitrary Command Injection

Synopsis

The remote web server hosts a CGI script that is affected by an arbitrary shell command execution vulnerability.

Description

According to its banner, the installed version of TWiki allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

See Also

http://www.nessus.org/u?b15c2dd7

Solution

Apply the appropriate hotfix listed in the vendor advisory.

Risk Factor

Medium

VPR Score

5.9

EPSS Score

0.0059

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	14960
CVE	CVE-2005-3056

Plugin Information

Published: 2005/10/20, Modified: 2024/06/05

Plugin Output

tcp/80/www

```
URL               : http://Epic-Metasploitable.epicode/twiki/bin/view
Installed version : 01 Feb 2003
Fixed version     : 04 Sep 2004 or apply the appropriate hotfix
```

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/80/www

```
The request GET /mutillidae/?page=<IMG%20SRC="javascript:alert(104);"> HTTP/1.1
Host: Epic-Metasploitable.epicode
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 :
<!-- Begin Content -->
<br />
<b>Warning</b>:  include(&lt;IMG SRC=&quot;javascript:alert(104);&quot;&
gt;) [<a href='function.include'>function.include</a>]: failed to open s
tream: No such file or directory in <b>/var/www/mutillidae/index.php</b>
 on line <b>469</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
```

```
The request GET /mutillidae/?page=/mutillidae/%00.html HTTP/1.1
Host: Epic-Metasploitable.epicode
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 :
<!-- Begin Content -->
<br />
<b>Warning</b>:  include(/mutillidae/) [<a href='function.include'>funct
ion.include</a>]: failed to open stream: No such file or directory in <b
>/var/www/mutillidae/index.php</b> on line <b>469</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]

The request GET /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template=company%00.html
 HTTP/1.1
Host: Epic-Metasploitable.epicode
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 :
<h1>TWiki Installation Error</h1>
Template file company..html.tmpl not found or tem [...]
```

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/80/www

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

  - http://Epic-Metasploitable.epicode/dvwa/login.php
  - http://Epic-Metasploitable.epicode/mutillidae/
  - http://Epic-Metasploitable.epicode/mutillidae/index.php
  - http://Epic-Metasploitable.epicode/phpMyAdmin/
  - http://Epic-Metasploitable.epicode/phpMyAdmin/index.php
  - http://Epic-Metasploitable.epicode/twiki/bin/search
  - http://Epic-Metasploitable.epicode/twiki/bin/search/Main
  - http://Epic-Metasploitable.epicode/twiki/bin/search/Main/SearchResult
  - http://Epic-Metasploitable.epicode/twiki/bin/view
  - http://Epic-Metasploitable.epicode/twiki/bin/view/Main
  - http://Epic-Metasploitable.epicode/twiki/bin/view/Main/WebHome
```

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/8180/www

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

  - http://Epic-Metasploitable.epicode:8180/admin/
  - http://Epic-Metasploitable.epicode:8180/admin/error.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/login.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/check.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colors.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/error/err.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/error/error.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/jsp2/el/functions.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/jsp2/el/implicit-objects.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/num/numguess.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/plugin/plugin.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/sessions/carts.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/sessions/carts.jsp
  - http://Epic-Metasploitable.epicode:8180/servlets-examples/servlet/CookieExample
  - http://Epic-Metasploitable.epicode:8180/servlets-examples/servlet/RequestParamExample
  - http://Epic-Metasploitable.epicode:8180/servlets-examples/servlet/SessionExample
```

88490 - Web Server Error Page Information Disclosure

Synopsis

The remote web server discloses information via a default error page.

Description

The default error page sent by the remote web server discloses information that can aid an attacker, such as the server version and languages used by the web server.

Solution

Modify the web server to not disclose detailed information about the underlying web server, or use a custom error page instead.

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: 2016/01/29, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Server Type    : Apache
Server Version : Apache/2.2.8
Source         : http://Epic-Metasploitable.epicode/H6KRPAcS
```

88490 - Web Server Error Page Information Disclosure

Synopsis

The remote web server discloses information via a default error page.

Description

The default error page sent by the remote web server discloses information that can aid an attacker, such as the server version and languages used by the web server.

Solution

Modify the web server to not disclose detailed information about the underlying web server, or use a custom error page instead.

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: 2016/01/29, Modified: 2022/04/11

Plugin Output

tcp/8180/www

```
Server Type    : Apache Tomcat
Server Version : 5.5
Source         : http://Epic-Metasploitable.epicode:8180/nz5n2Hil
```

10815 - Web Server Generic XSS

Synopsis

The remote web server is affected by a cross-site scripting vulnerability.

Description

The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. A remote attacker can exploit this issue, via a specially crafted request, to execute arbitrary HTML and script code in a user's browser within the security context of the affected site.

See Also

https://en.wikipedia.org/wiki/Cross-site_scripting

Solution

Contact the vendor for a patch or upgrade.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

3.8

EPSS Score

0.025

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

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

References

BID	5011
BID	5305

BID	7344
BID	7353
BID	8037
BID	14473
BID	17408
BID	54344
CVE	CVE-2002-1060
CVE	CVE-2002-1700
CVE	CVE-2003-1543
CVE	CVE-2005-2453
CVE	CVE-2006-1681
CVE	CVE-2012-3382
XREF	CWE:79

Plugin Information

Published: 2001/11/30, Modified: 2022/05/02

Plugin Output

tcp/8180/www

```
------------------------------ Request #1 ------------------------------

The full request used to detect this flaw was :

GET /admin/v3koglly.html HTTP/1.1
Host: <script>alert(Host)</script>:8180
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: JSESSIONID=15D765ABD1E85B74FF0F5FB7F8EC30BE
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, */*


The output was :

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Pragma: No-cache
Cache-Control: no-cache
Expires: Wed, 31 Dec 1969 19:00:00 GMT-05:00
Content-Type: text/html;charset=utf-8
Content-Length: 4759
Date: Mon, 10 Feb 2025 00:05:50 GMT
Connection: close

<head>
<title>Tomcat Server Administration</title>
<base href="http://<script>alert(Host)</script>:8180/admin/login.jsp">
<link rel="stylesheet" type="text/css" href="tree-control-test.css">
<link rel="stylesheet" type="text/css" href="admin.css">
```

88099 - Web Server HTTP Header Information Disclosure

Synopsis

The remote web server discloses information via HTTP headers.

Description

The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version and languages used by the web server.

Solution

Modify the HTTP headers of the web server to not disclose detailed information about the underlying web server.

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: 2016/01/22, Modified: 2019/04/30

Plugin Output

tcp/80/www

```
Server type     : Apache
Server version  : 2.2.8
Source          : 2.2.8
Additional data : X-Powered-By: PHP/5.2.4-2ubuntu5.10
```

11229 - Web Server info.php / phpinfo.php Detection

Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :

- The username of the user who installed PHP and if they are a SUDO user.

- The IP address of the host.

- The version of the operating system.

- The web server version.

- The root directory of the web server.

- Configuration information about the remote PHP installation.

Solution

Remove the affected file(s).

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: 2003/02/12, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
Nessus discovered the following URLs that call phpinfo() :

  - http://Epic-Metasploitable.epicode/phpinfo.php
```

```
    - http://Epic-Metasploitable.epicode/mutillidae/phpinfo.php
```

117334 - phpMyAdmin < 4.8.3 Vulnerability (PMASA-2018-5)

Synopsis

The remote web server hosts a PHP application that is affected by a cross-site Scripting vulnerability.

Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.3. It is, therefore, affected by a cross-site Scripting vulnerability.

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

See Also

https://www.phpmyadmin.net/security/PMASA-2018-5/

Solution

Upgrade to phpMyAdmin version 4.8.3 or later.

Alternatively, apply the patch referenced in the vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.0

EPSS Score

0.0019

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	105168
CVE	CVE-2018-15605

Plugin Information

Published: 2018/09/06, Modified: 2024/06/04

Plugin Output

tcp/80/www

```
URL               : http://Epic-Metasploitable.epicode/phpMyAdmin
Installed version : 3.1.1
Fixed version     : 4.8.3
```

129696 - phpMyAdmin <= 4.9.1 Cross-Site Request Forgery Vulnerability

Synopsis

The remote web server hosts a PHP application that is affected by a cross-site request forgery vulnerability

Description

A cross-site request forgery (XSRF) vulnerability exists in the Setup page of phpMyAdmin. A remote attacker can exploit this by tricking a user into visiting a specially crafted web page, allowing the attacker to delete any server in the setup page by creating a fake hyperlink containing the malicious request it wants the victim's web browser to execute.

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://www.phpmyadmin.net/files/4.9.1/

Solution

Upgrade to phpMyAdmin version 4.9.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.8069

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-12922
XREF	CWE:352

Plugin Information

Published: 2019/10/08, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
URL               : http://Epic-Metasploitable.epicode/phpMyAdmin
Installed version : 3.1.1
Fixed version     : 4.9.1
```

51425 - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)

Synopsis

The remote web server hosts a PHP script that is prone to a cross- site scripting attack.

Description

The version of phpMyAdmin fails to validate BBcode tags in user input to the 'error' parameter of the 'error.php' script before using it to generate dynamic HTML.

An attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user's browser to be executed within the security context of the affected site. For example, this could be used to cause a page with arbitrary text and a link to an external site to be displayed.

See Also

https://www.phpmyadmin.net/security/PMASA-2010-9/

Solution

Upgrade to phpMyAdmin 3.4.0-beta1 or later.

Risk Factor

Medium

VPR Score

3.8

EPSS Score

0.2301

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

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

References

BID	45633
CVE	CVE-2010-4480
XREF	EDB-ID:15699

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: 2011/01/06, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

  http://Epic-Metasploitable.epicode/phpMyAdmin/error.php?type=phpmyadmin_pmasa_2010_9.nasl&error=
%5ba%40https%3a%2f%2fwww.phpmyadmin.net%2fsecurity%2fPMASA-2010-9%2f%40_self%5dClick%20here%5b%2fa
%5d

It produced the following response :

<link rel="icon" href="./favicon.ico" type="image/x-icon" />
<link rel="shortcut icon" href="./favicon.ico" type="image/x-icon" />
<title>phpMyAdmin</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<style type="text/css">
```

49142 - phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)

Synopsis

The remote web server contains a PHP application that has a cross- site scripting vulnerability.

Description

The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user-supplied input to the 'verbose server name' field.

A remote attacker could exploit this by tricking a user into executing arbitrary script code.

See Also

https://www.tenable.com/security/research/tra-2010-02

https://www.phpmyadmin.net/security/PMASA-2010-7/

Solution

Upgrade to phpMyAdmin 3.3.7 or later.

Risk Factor

Medium

VPR Score

3.0

EPSS Score

0.0022

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

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

References

CVE	CVE-2010-3263
XREF	TRA:TRA-2010-02
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: 2010/09/08, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
By making a series of requests, Nessus was able to determine the
following phpMyAdmin installation is vulnerable :

  http://Epic-Metasploitable.epicode/phpMyAdmin/
```

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

2.2

EPSS Score

0.8939

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: 2024/10/07

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -3 seconds.
```

42983 - ISC BIND 9 DNSSEC Cache Poisoning

Synopsis

The remote name server is affected by a cache poisoning vulnerability.

Description

According to its version number, the remote installation of BIND suffers from a cache poisoning vulnerability. This issue affects all versions prior to 9.4.3-P5, 9.5.2-P2 or 9.6.1-P3.

Note that only nameservers that allow recursive queries and validate DNSSEC records are affected. Nessus has not attempted to verify if this configuration applies to the remote service, though, so this could be a false positive.

See Also

https://www.isc.org/advisories/CVE2009-4022

http://www.vupen.com/english/advisories/2010/1352

http://www.vupen.com/english/advisories/2010/0622

http://www.vupen.com/english/advisories/2009/3335

Solution

Upgrade to BIND 9.4.3-P5 / 9.5.2-P2 / 9.6.1-P3 or later.

Risk Factor

Low

VPR Score

5.9

EPSS Score

0.2545

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	37118
CVE	CVE-2009-4022
CVE	CVE-2010-0382
XREF	CERT:418861

Plugin Information

Published: 2009/12/02, Modified: 2018/06/27

Plugin Output

udp/53/dns

17811 - MySQL < 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 Client XSS

Synopsis

A remote database client have a cross-site scripting vulnerability.

Description

The version of MySQL installed on the remote host is earlier than 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 and thus does not properly encode angle brackets when 'mysql --html' option is used. Depending on how the output of the mysql client command is processed, the user may be vulnerable to cross-site scripting attacks.

See Also

https://bugs.mysql.com/bug.php?id=27884

Solution

Upgrade to MySQL version 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 or later.

Risk Factor

Low

VPR Score

3.8

EPSS Score

0.1054

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

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

References

BID	31486
CVE	CVE-2008-4456
XREF	CWE:79

Plugin Information

Published: 2012/01/16, Modified: 2018/11/15

Plugin Output

tcp/3306/mysql

```
Installed version : 5.0.51a-3ubuntu5
Fixed version     : 5.0.89
```

44080 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking

Synopsis

The remote SSH service may be affected by an X11 forwarding port hijacking vulnerability.

Description

According to its banner, the version of SSH installed on the remote host is older than 5.1 and may allow a local user to hijack the X11 forwarding port. The application improperly sets the 'SO_REUSEADDR' socket option when the 'X11UseLocalhost' configuration option is disabled.

Note that most operating systems, when attempting to bind to a port that has previously been bound with the 'SO_REUSEADDR' option, will check that either the effective user-id matches the previous bind (common BSD-derived systems) or that the bind addresses do not overlap (Linux and Solaris). This is not the case with other operating systems such as HP-UX.

See Also

https://www.openssh.com/txt/release-5.1

Solution

Upgrade to OpenSSH version 5.1 or later.

Risk Factor

Low

VPR Score

3.6

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	30339
CVE	CVE-2008-3259

XREF CWE:200

Plugin Information

Published: 2011/10/04, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 5.1
```

53841 - Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure

Synopsis

Local attackers may be able to access sensitive information.

Description

According to its banner, the version of OpenSSH running on the remote host is earlier than 5.8p2. Such versions may be affected by a local information disclosure vulnerability that could allow the contents of the host's private key to be accessible by locally tracing the execution of the ssh-keysign utility. Having the host's private key may allow the impersonation of the host.

Note that installations are only vulnerable if ssh-rand-helper was enabled during the build process, which is not the case for *BSD, OS X, Cygwin and Linux.

See Also

http://www.openssh.com/txt/portable-keysign-rand-helper.adv

http://www.openssh.com/txt/release-5.8p2

Solution

Upgrade to Portable OpenSSH 5.8p2 or later.

Risk Factor

Low

VPR Score

3.4

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	47691

CVE	CVE-2011-4327
XREF	Secunia:44347

Plugin Information

Published: 2011/05/09, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Installed version : 4.7p1
Fixed version     : 5.8p2
```

66970 - ProFTPD FTP Command Handling Symlink Arbitrary File Overwrite

Synopsis

The remote FTP server is affected by an arbitrary file overwrite vulnerability.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux. According to its banner, the version of ProFTPD installed on the remote host earlier than 1.3.4c. As such, it is potentially affected by a race condition error that does not securely create temporary files related to symlinks and newly created directories. A local, attacker could leverage this issue to overwrite arbitrary files and elevate privileges.

Note that Nessus did not actually test for the flaw but has instead relied on the version in ProFTPD's banner.

See Also

http://www.nessus.org/u?5fd455fb

http://proftpd.org/docs/RELEASE_NOTES-1.3.5rc1

http://bugs.proftpd.org/show_bug.cgi?id=3841

Solution

Upgrade to 1.3.4c / 1.3.5rc1 or apply the patch from the vendor.

Risk Factor

Low

VPR Score

3.6

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	57172
CVE	CVE-2012-6095

Plugin Information

Published: 2013/06/24, Modified: 2020/03/27

Plugin Output

tcp/2121/ftp

```
  Version source    : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
500 GET not understood
  Installed version : 1.3.1
  Fixed version     : 1.3.4c / 1.3.5rc1
```

86328 - SSH Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

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

Description

The remote SSH server allows connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time (depending on modulus size and attacker resources).

This allows an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

https://weakdh.org/

https://stribika.github.io/2015/01/04/secure-secure-shell.html

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

4.5

EPSS Score

0.9689

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: 2015/10/09, Modified: 2022/12/05

Plugin Output

tcp/22/ssh

```
The SSH server is vulnerable to the Logjam attack because :

  It supports diffie-hellman-group1-sha1 key
  exchange.

  It supports diffie-hellman-group-exchange-sha1
  key exchange and allows a moduli smaller than
  or equal to 1024.

Note that only an attacker with nation-state level resources
can effectively make use of the vulnerability, and only
against sessions where the vulnerable key exchange
algorithms are used.
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS v3.0 Base Score

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

VPR Score

6.5

EPSS Score

0.6016

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2023/10/27

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

https://datatracker.ietf.org/doc/html/rfc9142

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2024/03/22

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

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: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

Plugin Output

tcp/80/www

```
Page : /phpMyAdmin/
Destination Page: /phpMyAdmin/index.php

Page : /phpMyAdmin/index.php
Destination Page: /phpMyAdmin/index.php
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

Plugin Output

tcp/8180/www

```
Page : /admin/
Destination Page: /admin/j_security_check

Page : /admin/error.jsp
Destination Page: /admin/j_security_check
```

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

Plugin Output

tcp/80/www

```
Page : /phpMyAdmin/
Destination Page: /phpMyAdmin/index.php

Page : /phpMyAdmin/index.php
Destination Page: /phpMyAdmin/index.php
```

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

Plugin Output

tcp/8180/www

```
Page : /admin/
Destination Page: /admin/j_security_check

Page : /admin/error.jsp
Destination Page: /admin/j_security_check
```

34850 - Web Server Uses Basic Authentication Without HTTPS

Synopsis

The remote web server seems to transmit credentials in cleartext.

Description

The remote web server contains web pages that are protected by 'Basic'
authentication over cleartext.

An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

Solution

Make sure that HTTP authentication is transmitted over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

XREF	CWE:319
XREF	CWE:928
XREF	CWE:930
XREF	CWE:934

Plugin Information

Published: 2008/11/21, Modified: 2016/11/29

Plugin Output

tcp/8180/www

```
The following web pages use Basic Authentication over an unencrypted
channel :

/host-manager/html:/  realm="Tomcat Host Manager Application"
/manager/html:/  realm="Tomcat Manager Application"
/manager/status:/  realm="Tomcat Manager Application"
```

10407 - X Server Detection

Synopsis

An X11 server is listening on the remote host

Description

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

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: 2000/05/12, Modified: 2019/03/05

Plugin Output

tcp/6000/x11

```
X11 Version : 11.0
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2022/03/21

Plugin Output

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 8.04 (gutsy)
```

111465 - Apache HTTP Server Error Page Detection

Synopsis

The remote web server version can be obtained via a default error page.

Description

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

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/07/31, Modified: 2025/01/22

Plugin Output

tcp/80/www

```
Version : 2.2.8
Source  : Apache/2.2.8 (Ubuntu) DAV/2
URL     : http://Epic-Metasploitable.epicode/webmail/
```

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/80/www

```
URL        : http://Epic-Metasploitable.epicode/
Version    : 2.2.8
Source     : Server: Apache/2.2.8 (Ubuntu) DAV/2
backported : 0
modules    : DAV/2
os         : Ubuntu
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2024/11/14

Plugin Output

tcp/8180/www

```
URL        : http://Epic-Metasploitable.epicode:8180/
Version    : 5.5
backported : 0
source     : Apache Tomcat/5.5
```

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/8180/www

```
This web server was declared broken by :
 iplanet_dir_serv.nasl
for the following reason :
 The web server failed to respond at least 43 times for 4661 s.
```

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/80/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'topic' parameter of the /twiki/bin/view/Main/WebHome CGI :

/twiki/bin/view/Main/WebHome?topic=%00krjrai

-------- output --------
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title> TWiki . Main . krjrai   </title>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-88 [...]
<base href="http://Epic-Metasploitable.epicode/twiki/bin/view/Main [...]
------------------------

+ The 'search' parameter of the /twiki/bin/search/Main/SearchResult CGI :
```

```
/twiki/bin/search/Main/SearchResult?search=%00krjrai

-------- output --------
</tr>
</table>
</form>Search: <b> !krjrai </b>
<p /><table width="100%" border="0" cellpadding="0" cellspacing="4">
<tr bgcolor="#FFFFC0">
------------------------

+ The 'template' parameter of the /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company CGI :

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template=%00krj
rai

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file .krjrai.tmpl not found or template directory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=%00krjrai

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=.krjrai">Toggle Hints</a><
/td><td><a href="./index.php?do=toggle-security&page=.krjrai">Toggl
e Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------

+ The 'do' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?do=%00krjrai&do=toggle-hints

-------- output --------
Pragma: no-cache
Set-Cookie: showhints=0
Location: /mutillidae/index.php?do=%00krjrai&do=toggle-hints
Content-Length: 0
Keep-Alive: timeout=15, max=100
------ [...]
```

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/80/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]

on site request forgery                  : S=9          SP=9         AP=15        SC=4         AC=18

SQL injection                            : S=1073       SP=1073      AP=1885      SC=203
 AC=3335
unseen parameters                        : S=1295       SP=1295      AP=2275      SC=245
 AC=4025
local file inclusion                     : S=148        SP=148       AP=260       SC=28
 AC=460
cookie manipulation                      : S=10         SP=10        AP=10        SC=4         AC=10

web code injection                       : S=37         SP=37        AP=65        SC=7
 AC=115
XML injection                            : S=37         SP=37        AP=65        SC=7
 AC=115
format string                            : S=74         SP=74        AP=130       SC=14
 AC=230
script injection                         : S=9          SP=9         AP=15        SC=4         AC=18
```

```
injectable parameter                     : S=74         SP=74        AP=130       SC=14
 AC=230
cross-site scripting (comprehensive test): S=777        SP=777       AP=1365      SC=147
 AC=2415
cross-site scripting (extended patterns) : S=63         SP=63        AP=105       SC=28
 AC=126
directory traversal (write access)       : S=74         SP=74        AP=130       SC=14
 AC=230
SSI injection                            : S=111        SP=111       AP=195       SC=21
 AC=345
header injection                         : S=18         SP=18        AP=30        SC=8         AC=36

HTML injection                           : S=45         SP=45        AP=75        SC=20        AC=90

directory traversal                      : S=1073       SP=1073      AP=1885      SC=203
 AC=3335
cross-site scripting (quick test)      [...]
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :

'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.

- 'Stop after one flaw is found per web server (fastest)'

under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Risk Factor

None

Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following tests timed out without finding any flaw :
- SQL injection
- local file inclusion

The following tests were interrupted and did not report all possible flaws :
- blind SQL injection
- cross-site scripting (comprehensive test)
- arbitrary command execution
- directory traversal (extended test)
- directory traversal
```

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: 2025/02/06

Plugin Output

tcp/0

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

  cpe:/o:canonical:ubuntu_linux:8.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:tomcat:5.5 -> Apache Software Foundation Tomcat
  cpe:/a:isc:bind:9.4. -> ISC BIND
  cpe:/a:isc:bind:9.4.2 -> ISC BIND
  cpe:/a:mysql:mysql:5.0.51a-3ubuntu5 -> MySQL MySQL
  cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:4.7p1 -> OpenBSD OpenSSH
  cpe:/a:php:php:5.2.4 -> PHP PHP
  cpe:/a:php:php:5.2.4-2ubuntu5.10 -> PHP PHP
  cpe:/a:phpmyadmin:phpmyadmin:3.1.1 -> phpMYAdmin
  cpe:/a:postgresql:postgresql -> PostgreSQL
  cpe:/a:samba:samba:3.0.20 -> Samba Samba
```

```
    cpe:/a:twiki:twiki:01_feb_2003 -> TWiki
```

10028 - DNS Server BIND version Directive Remote Version Detection

Synopsis

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

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF	IAVT:0001-T-0583

Plugin Information

Published: 1999/10/12, Modified: 2022/10/12

Plugin Output

udp/53/dns

```
Version : 9.4.2
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

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: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53/dns

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

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: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53/dns

11951 - DNS Server Fingerprinting

Synopsis

It may be possible to fingerprint the remote DNS server.

Description

This script attempts to identify the remote DNS server type and version by sending various invalid requests to the remote DNS server and analyzing the error codes returned.

See Also

http://cr.yp.to/surveys/dns1.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/16, Modified: 2022/04/11

Plugin Output

udp/53/dns

```
The remote name server could be fingerprinted as being :

  ISC BIND 9.5.0
```

72779 - DNS Server Version Detection

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2024/09/24

Plugin Output

tcp/53/dns

```
DNS server answer for "version.bind" (over TCP) :

  9.4.2
```

35371 - DNS Server hostname.bind Map Hostname Disclosure

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

udp/53/dns

```
The remote host name is :

metasploitable
```

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: 2025-02-09 23:04:59
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 : 95
```

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/80/www

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


http://TWiki.org/                       - /twiki/bin/view/Main/WebHome
http://TWiki.org/cgi-bin/view/Main/TWikiAdminGroup - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/Main/TWikiUsers - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/AlWilliams - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/AndreaSterbini - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/BookView - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ChangePassword - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ChristopheVermeulen - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ColasNahaboo - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/CrisBailiff - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/DavidWarman - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/DontNotify - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/FileAttachment - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/FormattedSearch - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/HaroldGottschalk - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/InterwikiPlugin - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/JohnAltstadt - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/JohnTalintyre - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/KevinKinnell - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/KlausWriessnegger - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManagingTopics - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManagingWebs - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManpreetSingh - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/NewUserTemplate - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/NicholasLee - /twiki/TWikiHistory.html
http://TWiki.org/cgi- [...]
```

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/8180/www

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


http://Epic-Metasploitable.epicode:8180/admin/error.jsp - /admin/j_security_check
http://Epic-Metasploitable.epicode:8180/admin/login.jsp - /admin/
http://ant.apache.org                   - /tomcat-docs/manager-howto.html
http://ant.apache.org/bindownload.cgi   - /tomcat-docs/building.html
http://apache.apache.org/               - /tomcat-docs/appdev/index.html
http://apr.apache.org/                  - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_proxy_ajp.html - /tomcat-docs/config/ajp.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcacertificatefile - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcacertificatepath - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcarevocationfile - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcarevocationpath - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcertificatechainfile - /tomcat-docs/apr.html
http://httpd.apache.org/docs/howto/ssi.html#basicssidirectives - /tomcat-docs/ssi-howto.html
http://issues.apache.org/bugzilla/buglist.cgi?
bug_status=UNCONFIRMED&bug_status=NEW&bug_status=ASSIGNED&bug_status=REOPENED&bug_status=RESOLVED&resolution=LATER
&bugidtype=include&product=Tomcat+5&cmdtype=doit&order=Importance - /
http://issues.apache.org/bugzilla/show_bug.cgi?id=22679 - /tomcat-docs/ssl-howto.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=34643 - /tomcat-docs/ssl-howto.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=37668 - /tomcat-docs/config/context.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=38217 - /tomcat-docs/ssl-howto.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=39013 - /tomcat-docs/config/context.html
http://jakarta.apache.org/commons       - /tomcat-docs/jndi-resources-howto.html
http://jakarta.apache.org/commons/dbcp/configuration.html - /tomcat-doc [...]
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

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

Plugin Output

tcp/2121/ftp

```
The remote FTP banner is :

220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
```

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/80/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 :

    /dav

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

    /doc
    /dvwa/dvwa
    /dvwa/dvwa/css
    /dvwa/dvwa/images
    /dvwa/dvwa/includes
    /dvwa/dvwa/includes/DBMS
    /dvwa/dvwa/js
    /icons
    /mutillidae/documentation
    /mutillidae/styles
    /mutillidae/styles/ddsmoothmenu
    /test
    /test/testoutput
    /twiki


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
    /twiki/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 :

    /dav

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

    /
    /doc
    /dvwa
    /dvwa/dvwa
    /dvwa/dvwa/css
    /dvwa/dvwa/images
    /dvwa/dvwa/includes
    /dvwa/dvwa/includes/DBMS
    /dvwa/dvwa/js
    /icons
    /mutillidae
    /mutillidae/documentation
    /mutillidae/styles
    /mutillidae/styles/ddsmoothmenu
    /phpMyAdmin
    /test
    /test/testoutput
    /twiki

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
    /dav
```

```
    /twiki/bin
```

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/8180/www

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

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

    /admin/error.jsp
    /host-manager
    /jsp-examples
    /jsp-examples/cal
    /jsp-examples/checkbox
    /jsp-examples/colors
    /jsp-examples/dates
    /jsp-examples/error
    /jsp-examples/forward
    /jsp-examples/include
    /jsp-examples/jsp2
    /jsp-examples/jsp2/el
    /jsp-examples/jsp2/jspattribute
    /jsp-examples/jsp2/jspx
    /jsp-examples/jsp2/misc
    /servlets-examples


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /admin
    /admin/error.jsp
    /host-manager
    /jsp-examples
    /jsp-examples/cal
    /jsp-examples/checkbox
    /jsp-examples/colors
    /jsp-examples/dates
    /jsp-examples/error
    /jsp-examples/forward
    /jsp-examples/include
    /jsp-examples/jsp2
    /jsp-examples/jsp2/el
    /jsp-examples/jsp2/jspattribute
    /jsp-examples/jsp2/jspx
    /jsp-examples/jsp2/misc
    /servlets-examples
```

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/80/www

```
The remote web server type is :

Apache/2.2.8 (Ubuntu) DAV/2
```

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/8180/www

```
The remote web server type is :

Apache-Coyote/1.1
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
192.168.51.101 resolves as Epic-Metasploitable.epicode.
```

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/80/www

```
Response Code : HTTP/1.1 200 OK

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

  Date: Mon, 10 Feb 2025 00:03:20 GMT
  Server: Apache/2.2.8 (Ubuntu) DAV/2
  X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html

Response Body :

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _       ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
```

```
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                             |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

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/8180/www

```
Response Code : HTTP/1.1 200 OK

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

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=ISO-8859-1
  Date: Mon, 10 Feb 2025 00:03:19 GMT
  Connection: close

Response Body :

<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0
```

```
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
    <head>
    <title>Apache Tomcat/5.5</title>
    <style type="text/css">
    /*<![CDATA[*/
      body {
          color: #000000;
          background-color: #FFFFFF;
  font-family: Arial, "Times New Roman", Times, serif;
          margin: 10px 0px;
      }

    img {
       border: none;
    }

    a:link, a:visited {
        color: blue
    }

    th {
        font-family: Verdana, "Times New Roman", Times, serif;
        font-size: 110%;
        font-weight: normal;
        font-style: italic;
        background: #D2A41C;
        text-align: left;
    }

    td {
        color: #000000;
font-family: Arial, Helvetica, sans-serif;
    }

    td.men [...]
```

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
6TCP
17UDP
58IPv6-ICMP
132SCTP
136UDPLite
```

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Here is the browse list of the remote host :

METASPLOITABLE ( os : 0.0 )
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- Guest account

- Supplied credentials

See Also

http://www.nessus.org/u?5c2589f6

https://support.microsoft.com/en-us/help/246261

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2024/12/06

Plugin Output

tcp/445/cifs

```
- NULL sessions may be enabled on the remote host.
```

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 : Unix
The remote native LAN manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE
```

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
```

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 does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
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/80/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://Epic-Metasploitable.epicode/
  - http://Epic-Metasploitable.epicode/dav/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/DBMS.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/MySQL.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPage.inc.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPhpIds.inc.php
```

```
   - http://Epic-Metasploitable.epicode/dvwa/dvwa/js/
   - http://Epic-Metasploitable.epicode/dvwa/login.php
   - http://Epic-Metasploitable.epicode/mutillidae/
   - http://Epic-Metasploitable.epicode/mutillidae/documentation/
   - http://Epic-Metasploitable.epicode/mutillidae/documentation/how-to-access-Mutillidae-over-
Virtual-Box-network.php
   - http://Epic-Metasploitable.epicode/mutillidae/documentation/vulnerabilities.php
   - http://Epic-Metasploitable.epicode/mutillidae/framer.html
   - http://Epic-Metasploitable.epicode/mutillidae/index.php
   - http://Epic-Metasploitable.epicode/mutillidae/set-up-database.php
   - http://Epic-Metasploitable.epicode/mutillidae/styles/
   - http://Epic-Metasploitable.epicode/mutillidae/styles/ddsmoothmenu/
   - http://Epic-Metasploitable.epicode/phpMyAdmin/
   - http://Epic-Metasploitable.epicode/phpMyAdmin/index.php
   - http://Epic-Metasploitable.epicode/test/
   - http://Epic-Metasploitable.epicode/test/testoutput/
   - http://Epic-Metasploitable.epicode/twiki/
   - http://Epic-Metasploitable.epicode/twiki/TWikiHistory.html
   - http://Epic-Metasploitable.epicode/twiki/bin/oops
   - http://Epic-Metasploitable.epicode/twiki/bin/oops/Main
   - http://Epic-Metasploitable.epicode/twiki/bin/oops/Main/WebHomemailto%3Awebmastery [...]
```

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/8180/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://Epic-Metasploitable.epicode:8180/
  - http://Epic-Metasploitable.epicode:8180/admin/
  - http://Epic-Metasploitable.epicode:8180/admin/error.jsp
  - http://Epic-Metasploitable.epicode:8180/admin/j_security_check
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entries.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entry.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/TableBean.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal2.jsp.html
```

```
- http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/calendar.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/login.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/CheckTest.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/check.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/cresult.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/ColorGameBean.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/clr.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colors.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp.html
- http://Epic-Metasploitable.e [...]
```

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/80/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://Epic-Metasploitable.epicode/
  - http://Epic-Metasploitable.epicode/dav/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/DBMS.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/MySQL.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPage.inc.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPhpIds.inc.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/js/
  - http://Epic-Metasploitable.epicode/dvwa/login.php
  - http://Epic-Metasploitable.epicode/mutillidae/
  - http://Epic-Metasploitable.epicode/mutillidae/documentation/
```

```
  - http://Epic-Metasploitable.epicode/mutillidae/documentation/how-to-access-Mutillidae-over-
Virtual-Box-network.php
  - http://Epic-Metasploitable.epicode/mutillidae/documentation/vulnerabilities.php
  - http://Epic-Metasploitable.epicode/mutillidae/framer.html
  - http://Epic-Metasploitable.epicode/mutillidae/index.php
  - http://Epic-Metasploitable.epicode/mutillidae/set-up-database.php
  - http://Epic-Metasploitable.epicode/mutillidae/styles/
  - http://Epic-Metasploitable.epicode/mutillidae/styles/ddsmoothmenu/
  - http://Epic-Metasploitable.epicode/phpMyAdmin/
  - http://Epic-Metasploitable.epicode/phpMyAdmin/index.php
  - http://Epic-Metasploitable.epicode/test/
  - http://Epic-Metasploitable.epicode/test/testoutput/
  - http://Epic-Metasploitable.epicode/twiki/
  - http://Epic-Metasploitable.epicode/twiki/TWikiHistory.html
  - http://Epic-Metasploitable.epicode/twiki/bin/oops
  - http://Epic-Metasploitable.epicode/twiki/bin/oops/Main
  - http://Epic-Metasploitable.epicode/twiki/bin/oops/Main/WebHomemailto%3Awebmasteryour
  - http://Epic-Meta [...]
```

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/8180/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://Epic-Metasploitable.epicode:8180/
  - http://Epic-Metasploitable.epicode:8180/admin/
  - http://Epic-Metasploitable.epicode:8180/admin/error.jsp
  - http://Epic-Metasploitable.epicode:8180/admin/j_security_check
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entries.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entry.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/TableBean.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal2.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/calendar.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/login.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/CheckTest.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/check.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp
```

```
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/cresult.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/ColorGameBean.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/clr.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colors.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples [...]
```

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0802

Plugin Information

Published: 2001/08/13, Modified: 2022/10/12

Plugin Output

tcp/3306/mysql

```
Version  : 5.0.51a-3ubuntu5
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_SSL (Switch to SSL after handshake)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

10437 - NFS Share Export List

Synopsis

The remote NFS server exports a list of shares.

Description

This plugin retrieves the list of NFS exported shares.

See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Solution

Ensure each share is intended to be exported.

Risk Factor

None

Plugin Information

Published: 2000/06/07, Modified: 2019/10/04

Plugin Output

tcp/2049/rpc-nfs

```
Here is the export list of Epic-Metasploitable.epicode :
  / *
```

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: 2024/12/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202502091911
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : W12D4 - Second Scan --> Metasploitable
```

```
Scan policy used : Copy of Basic Network Scan
Scanner IP : 192.168.50.100
Port scanner(s) : nessus_tcp_scanner
Port range : 1-65535
Ping RTT : 54.562 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 2
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_combinations
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 : 2
Max checks : 2
Recv timeout : 15
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/2/9 23:41 CET (UTC +01:00)
Scan duration : 17083 sec
Scan for malware : no
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/25/smtp

```
Port 25/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/53/dns

```
Port 53/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/80/www

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

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/111/rpc-portmapper

```
Port 111/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/1099/rmi_registry

```
Port 1099/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/2049/rpc-nfs

```
Port 2049/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/2121/ftp

```
Port 2121/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/3306/mysql

```
Port 3306/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/3632

```
Port 3632/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/5432/postgresql

```
Port 5432/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/5900/vnc

```
Port 5900/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/6000/x11

```
Port 6000/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/8009

```
Port 8009/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/8180/www

```
Port 8180/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/8787

```
Port 8787/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/34504/rpc-nlockmgr

```
Port 34504/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/35214/rmi_registry

```
Port 35214/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/58801/rpc-status

```
Port 58801/tcp was found to be open
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/60957/rpc-mountd

```
Port 60957/tcp was found to be open
```

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: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Confidence level : 95
Method : HTTP

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
ICMP:!::1:1:0:64:1:64:1:0:::0::1:>64:64:0:1:1:2:1:1:1:1:0:64:5792:MSTNW:5:1:1
SinFP:
   P1:B10113:F0x12:W5840:O0204ffff:M1460:
   P2:B10113:F0x12:W5792:O0204ffff0402080affffffff4445414401030305:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191003_7_p=2121R
SMTP:!:220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple
 Affairss/CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple
 Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple Affairss/
CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple Affairs
ed093088706603bfd5dc237399b498da2d4d31c6



The remote host is running Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
```

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 SSH 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: 2025/02/06

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 4.7p1
Banner  : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

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/25/smtp

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/5432/postgresql

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: 2025/01/31

Plugin Output

tcp/80/www

```
Nessus was able to identify the following PHP version information :

  Version : 5.2.4-2ubuntu5.10
  Source  : X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Source  : http://Epic-Metasploitable.epicode/phpinfo.php
```

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: 2025/01/14

Plugin Output

tcp/0

```
. You need to take the following 14 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 78 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-2016-8743, CVE-2016-5387, CVE-2016-4975, 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-2011-3348, CVE-2011-3192
CVE-2011-0419, CVE-2010-2068, CVE-2010-1623, CVE-2010-1452, CVE-2010-0434
CVE-2010-0425, CVE-2010-0408, CVE-2009-3720, CVE-2009-3560, CVE-2009-3555
CVE-2009-3095, CVE-2009-3094, CVE-2009-2699, CVE-2009-2412, CVE-2009-1956
CVE-2009-1955, CVE-2009-1891, CVE-2009-1890, CVE-2009-1195, CVE-2009-1191
CVE-2009-0023, CVE-2007-6750, CVE-2006-20001
```

```
[ ISC BIND 9.0.0 < 9.16.48 / 9.9.3-S1 < 9.16.48-S1 / 9.18.0 < 9.18.24 / 9.18.11-S1 < 9.18.24-S1 /
 9.19.0 < 9.19.21 Vulnerability (cve-2023-50387) (190444) ]

+ Action to take : Upgrade to ISC BIND version 9.16.48 / 9.16.48-S1 / 9.18.24 / 9.18.24-S1 / 9.19.21
 or later.

+ Impact : Taking this action will resolve the following 36 different vulnerabilities :
CVE-2023-50387, CVE-2023-3341, CVE-2022-2795, CVE-2021-25219, CVE-2021-25215
CVE-2020-8622, CVE-2020-8617, CVE-2020-8616, CVE-2018-5741, CVE-2017-3141
CVE-2017-3140, CVE-2016-9778, CVE-2016-9444, CVE-2016-9147, CVE-2016-9131
CVE-2016-8864, CVE-201 [...]
```

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2024/03/25

Plugin Output

tcp/0

```
The remote host is up
The remote host replied to an ICMP echo packet
```

118224 - PostgreSQL STARTTLS Support

Synopsis

The remote service supports encrypting traffic.

Description

The remote PostgreSQL server supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.

See Also

https://www.postgresql.org/docs/9.2/protocol-flow.html#AEN96066

https://www.postgresql.org/docs/9.2/protocol-message-formats.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/10/19, Modified: 2022/04/11

Plugin Output

tcp/5432/postgresql

```
Here is the PostgreSQL's SSL certificate that Nessus
was able to collect after sending a pre-login packet :

------------------------------ snip ------------------------------
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
```

```
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75


------------------------------ snip ------------ [...]
```

26024 - PostgreSQL Server Detection

Synopsis

A database service is listening on the remote host.

Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

See Also

https://www.postgresql.org/

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2007/09/14, Modified: 2023/05/24

Plugin Output

tcp/5432/postgresql

110976 - PostgreSQL Unauthenticated Version Detection

Synopsis

It was possible to gather database version information from an error message.

Description

It was possible to guess the remote PostgreSQL database version from a unique error message.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/07/10, Modified: 2025/01/13

Plugin Output

tcp/5432/postgresql

```
Source  : Fauth.c.L1003.Rauth_failed
Version : 8.3.8
```

40665 - Protected Web Page Detection

Synopsis

Some web pages require authentication.

Description

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :

- Basic is the simplest, but the credentials are sent in cleartext.

- NTLM provides an SSO in a Microsoft environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.

- Digest is a cryptographically strong scheme. Credentials are never sent in cleartext, although they may still be cracked by a dictionary attack.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/08/21, Modified: 2016/10/04

Plugin Output

tcp/8180/www

```
The following pages are protected by the Basic authentication scheme :

/host-manager/html
/manager/html
/manager/status
```

22227 - RMI Registry Detection

Synopsis

An RMI registry is listening on the remote host.

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html

http://www.nessus.org/u?b6fd7659

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/08/16, Modified: 2022/06/01

Plugin Output

tcp/1099/rmi_registry
tcp/1099/rmi_registry

```
Valid response recieved for port 1099:
0x00:  51 AC ED 00 05 77 0F 01 60 C4 91 FD 00 00 01 94    Q....w..`.......
0x10:  ED 4A 5B 37 80 02 75 72 00 13 5B 4C 6A 61 76 61    .J[7..ur..[Ljava
0x20:  2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56    .lang.String;..V
0x30:  E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00       ...{G...pxp....
```

22227 - RMI Registry Detection

Synopsis

An RMI registry is listening on the remote host.

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html

http://www.nessus.org/u?b6fd7659

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/08/16, Modified: 2022/06/01

Plugin Output

tcp/35214/rmi_registry
tcp/35214/rmi_registry

```
Valid response recieved for port 35214:
0x00:  51 AC ED 00 05 77 0F 01 60 C4 91 FD 00 00 01 94    Q....w..`.......
0x10:  ED 4A 5B 30 80 02 75 72 00 13 5B 4C 6A 61 76 61    .J[0..ur..[Ljava
0x20:  2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56    .lang.String;..V
0x30:  E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00       ...{G...pxp....
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/111/rpc-portmapper

```
The following RPC services are available on TCP port 111 :

 - program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/111/rpc-portmapper

```
The following RPC services are available on UDP port 111 :

 - program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/2049/rpc-nfs

```
The following RPC services are available on TCP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/2049/rpc-nfs

```
The following RPC services are available on UDP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/34504/rpc-nlockmgr

```
The following RPC services are available on TCP port 34504 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/36117/rpc-mountd

```
The following RPC services are available on UDP port 36117 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/40018/rpc-nlockmgr

```
The following RPC services are available on UDP port 40018 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/58801/rpc-status

```
The following RPC services are available on TCP port 58801 :

 - program: 100024 (status), version: 1
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/60887/rpc-status

```
The following RPC services are available on UDP port 60887 :

 - program: 100024 (status), version: 1
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/60957/rpc-mountd

```
The following RPC services are available on TCP port 60957 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
```

53335 - RPC portmapper (TCP)

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/04/08, Modified: 2011/08/29

Plugin Output

tcp/111/rpc-portmapper

10223 - RPC portmapper Service Detection

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0632

Plugin Information

Published: 1999/08/19, Modified: 2019/10/04

Plugin Output

udp/111/rpc-portmapper

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/25/smtp

```
Remote SMTP server banner :

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

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

https://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

Plugin Output

tcp/25/smtp

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
```

```
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

------------------------------ snip --------- [...]
```

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: 2025/01/20

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :

  Client to Server: aes256-ctr
  Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
```

```
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

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: 2024/07/24

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-sha1-96

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96
```

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: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password
```

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/25/smtp

```
This port supports SSLv2/SSLv3/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/5432/postgresql

```
This port supports SSLv3/TLSv1.0.
```

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/25/smtp

```
The host names known by Nessus are :

  epic-metasploitable.epicode
  metasploitable

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

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/5432/postgresql

```
The host names known by Nessus are :

  epic-metasploitable.epicode
  metasploitable

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

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/25/smtp

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
                     83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D [...]
```

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/5432/postgresql

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
                     83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D [...]
```

25240 - Samba Server Detection

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

https://www.samba.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2022/10/12

Plugin Output

tcp/445/cifs

104887 - Samba Version

Synopsis

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/11/30, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote Samba Version is : Samba 3.0.20-Debian
```

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/25/smtp

```
An SMTP 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/80/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/2121/ftp

```
An FTP 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/5900/vnc

```
A vnc 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/8180/www

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

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

Plugin Output

tcp/3306/mysql

```
A MySQL 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

19941 - TWiki Detection

Synopsis

The remote web server hosts a Wiki system written in Perl.

Description

The remote host is running TWiki, an open source wiki system written in Perl.

See Also

http://twiki.org

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/10/06, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL     : http://Epic-Metasploitable.epicode/twiki/bin/view
Version : 01 Feb 2003
```

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

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

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 192.168.50.100 to 192.168.51.101 :
192.168.50.100
192.168.50.1
192.168.51.101

Hop Count: 2
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/8787

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port    : 8787
  Type    : get_http
  Banner :
0x0000:  00 00 00 03 04 08 46 00 00 03 A1 04 08 6F 3A 16    ......F......o:.
           0x0010:  44 52 62 3A 3A 44 52 62 43 6F 6E 6E 45 72 72 6F    DRb::DRbConnErro
           0x0020:  72 07 3A 07 62 74 5B 17 22 2F 2F 75 73 72 2F 6C    r.:.bt[."//usr/l
           0x0030:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    ib/ruby/1.8/drb/
           0x0040:  64 72 62 2E 72 62 3A 35 37 33 3A 69 6E 20 60 6C    drb.rb:573:in `l
           0x0050:  6F 61 64 27 22 37 2F 75 73 72 2F 6C 69 62 2F 72    oad'"7/usr/lib/r
           0x0060:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2E    uby/1.8/drb/drb.
           0x0070:  72 62 3A 36 31 32 3A 69 6E 20 60 72 65 63 76 5F    rb:612:in `recv_
           0x0080:  72 65 71 75 65 73 74 27 22 37 2F 75 73 72 2F 6C    request'"7/usr/l
           0x0090:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    ib/ruby/1.8/drb/
           0x00A0:  64 72 62 2E 72 62 3A 39 31 31 3A 69 6E 20 60 72    drb.rb:911:in `r
           0x00B0:  65 63 76 5F 72 65 71 75 65 73 74 27 22 3C 2F 75    ecv_request'"</u
           0x00C0:  73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F    sr/lib/ruby/1.8/
           0x00D0:  64 72 62 2F 64 72 62 2E 72 62 3A 31 35 33 30 3A    drb/drb.rb:1530:
           0x00E0:  69 6E 20 60 69 6E 69 74 5F 77 69 74 68 5F 63 6C    in `init_with_cl
           0x00F0:  69 65 6E 74 27 22 39 2F 75 73 72 2F 6C 69 62 2F    ient'"9/usr/lib/
           0x0100:  72 75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62    ruby/1.8/drb/drb
           0x0110:  2E 72 62 3A 31 35 34 32 3A 69 6E 20 60 73 65 74    .rb:1542:in `set
           0x0120:  75 70 5F 6D 65 73 73 61 67 65 27 22 33 2F 75 73    up_message'"3/us
           0x0130:  72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64    r/lib/ruby/1.8/d
           0x0140:  72 62 2F 64 72 62 2E 72 62 3A 31 34 39 34  [...]
```

19288 - VNC Server Security Type Detection

Synopsis

A VNC server is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types'.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/07/22, Modified: 2021/07/13

Plugin Output

tcp/5900/vnc

```
\nThe remote VNC server chose security type #2 (VNC authentication)
```

65792 - VNC Server Unencrypted Communication Detection

Synopsis

A VNC server with one or more unencrypted 'security-types' is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/03, Modified: 2014/03/12

Plugin Output

tcp/5900/vnc

```
The remote VNC server supports the following security type
which does not perform full data communication encryption :

  2 (VNC authentication)
```

10342 - VNC Software Detection

Synopsis

The remote host is running a remote display software (VNC).

Description

The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

See Also

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

Solution

Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 2000/03/07, Modified: 2017/06/12

Plugin Output

tcp/5900/vnc

```
The highest RFB protocol version supported by the server is :

  3.3
```

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: 2025/02/06

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

72771 - Web Accessible Backups

Synopsis

The remote web server hosts web-accessible backups or archives.

Description

The remote web server is hosting web-accessible archive files that may contain backups or sensitive data.

Solution

Review each of the files and ensure they are in compliance with your security policy.

Risk Factor

None

Plugin Information

Published: 2014/03/03, Modified: 2022/04/11

Plugin Output

tcp/8180/www

```
Nessus was able to identify the following archive file on the
remote web server :

ZIP Archive :
   http://Epic-Metasploitable.epicode:8180/tomcat-docs/appdev/sample/sample.war
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/80/www

```
The following cookies are expired :

Name : pma_fontsize
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Sun, 11-Feb-2024 00:08:10 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_collation_connection
Path : /phpMyAdmin/
Value : deleted
```

```
Domain :
Version : 1
Expires : Sun, 11-Feb-2024 00:09:57 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Sun, 11-Feb-2024 00:08:06 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/8180/www

```
The following cookies are expired :

Name : pma_fontsize
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Sun, 11-Feb-2024 00:08:10 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_collation_connection
Path : /phpMyAdmin/
Value : deleted
```

```
Domain :
Version : 1
Expires : Sun, 11-Feb-2024 00:09:57 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Sun, 11-Feb-2024 00:08:06 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

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/80/www

```
The following cookies do not set the HttpOnly cookie flag :

Name : JSESSIONID
Path : /admin
Value : F92B035EFB7CF20FB6D5B99C5C55C520
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 3D780737A3857F1972080BEDFDA92456
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : ec92715f0d2a9da29d2282c615450c93
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : FABCE0CB99995F5261659C8386AA7E47
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

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/8180/www

```
The following cookies do not set the HttpOnly cookie flag :

Name : JSESSIONID
Path : /admin
Value : F92B035EFB7CF20FB6D5B99C5C55C520
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 3D780737A3857F1972080BEDFDA92456
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : ec92715f0d2a9da29d2282c615450c93
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : FABCE0CB99995F5261659C8386AA7E47
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
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/80/www

```
The following cookies do not set the secure cookie flag :

Name : JSESSIONID
Path : /admin
Value : F92B035EFB7CF20FB6D5B99C5C55C520
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : original
Domain :
Version : 1
Expires : Tue, 11-Mar-2025 23:45:59 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_fontsize
Path : /phpMyAdmin/
Value : 82%25
Domain :
Version : 1
Expires : Tue, 11-Mar-2025 23:45:59 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 3D780737A3857F1972080BEDFDA92456
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : ec92715f0d2a9da29d2282c615450c93
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : phpMyAdmin
Path : /phpMyAdmin/
Value : 973fe04b24d3b691722ab65500693cc14ef01b54
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_lang
Path : /phpMyAdmin/
Value : en-utf-8
Domain :
Version : 1
Expires : Tue, 11-Mar-2025 23:45:59 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_charset
Path : /phpMyAdmin/
Value : utf-8
Domain :
Version : 1
Expires : Tue, 11-Mar-2025 23:45:59 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : FABCE0CB99995F5261659C8386AA7E47
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
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/8180/www

```
The following cookies do not set the secure cookie flag :

Name : JSESSIONID
Path : /admin
Value : F92B035EFB7CF20FB6D5B99C5C55C520
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : original
Domain :
Version : 1
Expires : Tue, 11-Mar-2025 23:45:59 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_fontsize
Path : /phpMyAdmin/
Value : 82%25
Domain :
Version : 1
Expires : Tue, 11-Mar-2025 23:45:59 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 3D780737A3857F1972080BEDFDA92456
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : ec92715f0d2a9da29d2282c615450c93
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : phpMyAdmin
Path : /phpMyAdmin/
Value : 973fe04b24d3b691722ab65500693cc14ef01b54
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_lang
Path : /phpMyAdmin/
Value : en-utf-8
Domain :
Version : 1
Expires : Tue, 11-Mar-2025 23:45:59 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_charset
Path : /phpMyAdmin/
Value : utf-8
Domain :
Version : 1
Expires : Tue, 11-Mar-2025 23:45:59 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : FABCE0CB99995F5261659C8386AA7E47
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

40773 - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Potentially sensitive parameters for CGI /dvwa/login.php :

password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
```

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/80/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://Epic-Metasploitable.epicode/
  - http://Epic-Metasploitable.epicode/dav/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/help.css
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/login.css
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/main.css
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/source.css
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/RandomStorm.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/dollar.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/lock.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/login_logo.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/logo.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/spanner.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/warning.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/DBMS.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/MySQL.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPage.inc.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPhpIds.inc.php
```

```
   - http://Epic-Metasploitable.epicode/dvwa/dvwa/js/
   - http://Epic-Metasploitable.epicode/dvwa/dvwa/js/dvwaPage.js
   - http://Epic-Metasploitable.epicode/dvwa/login.php
   - http://Epic-Metasploitable.epicode/mutillidae/
   - http://Epic-Metasploitable.epicode/mutillidae/documentation/
   - http://Epic-Metasploitable.epicode/mutillidae/documentation/Mutillidae-Test-Scripts.txt
   - http://Epic-Metasploitable.epicode/mutillidae/documentation/how-to-access-Mutillidae-over-
Virtual-Box-network.php
   - http://Epic-Metasploitable.epicode/mutillidae/documentation/mutillid [...]
```

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/8180/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://Epic-Metasploitable.epicode:8180/
  - http://Epic-Metasploitable.epicode:8180/RELEASE-NOTES.txt
  - http://Epic-Metasploitable.epicode:8180/admin/
  - http://Epic-Metasploitable.epicode:8180/admin/error.jsp
  - http://Epic-Metasploitable.epicode:8180/admin/j_security_check
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entries.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entry.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/TableBean.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal2.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/calendar.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/login.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/CheckTest.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/check.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/cresult.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/ColorGameBean.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/clr.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colors.html
```

```
    - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp
    - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp.html
    - http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.html
    - http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp
    - http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp.html
    [...]
```

20108 - Web Server / Application favicon.ico Vendor Fingerprinting

Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

Description

The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

Solution

Remove the 'favicon.ico' file or create a custom one for your site.

Risk Factor

None

Plugin Information

Published: 2005/10/28, Modified: 2020/06/12

Plugin Output

tcp/8180/www

```
MD5 fingerprint : 4644f2d45601037b8423d45e13194c93
Web server      : Apache Tomcat or Alfresco Community
```

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/80/www

```
The following directories were discovered:
/cgi-bin, /doc, /test, /icons, /phpMyAdmin, /twiki/bin

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
```

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/8180/www

```
The following directories were discovered:
/admin, /jsp-examples, /servlets-examples

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

The following directories require authentication:
/host-manager/html, /manager/html
```

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

Plugin Output

tcp/80/www

```
The following email address has been gathered :

- 'SomeWikiName@somewhere.test', referenced from :
   /twiki/TWikiHistory.html
```

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

Plugin Output

tcp/8180/www

```
The following email addresses have been gathered :


- 'craigmcc@apache.org', referenced from :
   /tomcat-docs/appdev/printer/index.html
   /tomcat-docs/appdev/index.html
   /tomcat-docs/appdev/
   /tomcat-docs/appdev/printer/

- 'yoavs@apache.org', referenced from :
   /tomcat-docs/architecture/printer/
   /tomcat-docs/architecture/index.html
   /tomcat-docs/architecture/printer/index.html
   /tomcat-docs/architecture/

- 'users@tomcat.apache.org', referenced from :
   /

- 'jfarcand@apache.org', referenced from :
   /tomcat-docs/architecture/
   /tomcat-docs/architecture/printer/index.html
   /tomcat-docs/architecture/printer/
   /tomcat-docs/architecture/index.html

- 'fhanik@apache.org', referenced from :
   /tomcat-docs/architecture/printer/index.html
   /tomcat-docs/architecture/
   /tomcat-docs/architecture/printer/
   /tomcat-docs/architecture/index.html
```

```
 - 'dev@tomcat.apache.org', referenced from :
    /
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

tcp/8180/www

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /tomcat-docs/architecture/requestProcess/requestProcess.pdf
    /tomcat-docs/architecture/startup/serverStartup.pdf
```

11422 - Web Server Unconfigured - Default Install Page Present

Synopsis

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

Description

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

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8180/www

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

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: 2025/01/13

Plugin Output

tcp/80/www

```
Webmirror performed 100 queries in 7s (14.0285 queries per second)

The following CGIs have been discovered :


+ CGI : /phpMyAdmin/phpmyadmin.css.php
  Methods : GET
  Argument : js_frame
   Value: right
  Argument : nocache
   Value: 2457687233
  Argument : token
   Value: cf11a17fc0ebb6468a05dbea2f5c55c5


+ CGI : /phpMyAdmin/index.php
  Methods : POST
  Argument : db
  Argument : lang
  Argument : pma_password
  Argument : pma_username
  Argument : server
   Value: 1
  Argument : table
  Argument : token
   Value: cf11a17fc0ebb6468a05dbea2f5c55c5
```

```
+ CGI : /mutillidae/index.php
  Methods : GET
  Argument : do
   Value: toggle-security
  Argument : page
   Value: notes.php
  Argument : username
   Value: anonymous


+ CGI : /mutillidae/
  Methods : GET
  Argument : page
   Value: source-viewer.php


+ CGI : /rdiff/TWiki/TWikiHistory
  Methods : GET
  Argument : rev1
   Value: 1.8
  Argument : rev2
   Value: 1.7


+ CGI : /view/TWiki/TWikiHistory
  Methods : GET
  Argument : rev
   Value: 1.7


+ CGI : /oops/TWiki/TWikiHistory
  Methods : GET
  Argument : param1
   Value: 1.10
  Argument : template
   Value: oopsrev


+ CGI : /twiki/bin/view/Main/WebHome
  Methods : GET
  Argument : topic


+ CGI : /twiki/bin/search/Main/SearchResult
  Methods : GET
  Argument : search


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/edit/Main/WebHome
  Methods : GET
  Argument : t
   Value: 1739144762


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/search/Main/SearchResult
  Methods : GET
  Argument : regex
   Value: on
  Argument : scope
   Value: text
  Argument : search
   Value: Web%20*Home%5B%5EA-Za-z%5D


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/view/Main/WebHome
  Methods : GET
  Argument : rev
   Value: 1.18
  Argument : skin
```

```
    Value: print


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/rdiff/Main/WebHome
  Methods : GET
  Argument : rev1
    Value: 1.19
  Argument : rev2
    Value: 1.18


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/oops/Main/WebHome
  Methods : GET
  Argument : param1
    Value: 1.20
  Argum [...]
```

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: 2025/01/13

Plugin Output

tcp/8180/www

```
Webmirror performed 551 queries in 63s (8.0746 queries per second)

The following CGIs have been discovered :


+ CGI : /jsp-examples/jsp2/el/implicit-objects.jsp
  Methods : GET
  Argument : foo
   Value: bar


+ CGI : /jsp-examples/jsp2/el/functions.jsp
  Methods : GET
  Argument : foo
   Value: JSP+2.0


+ CGI : /admin/j_security_check
  Methods : POST
  Argument : j_password
  Argument : j_username


+ CGI : /jsp-examples/num/numguess.jsp
  Methods : GET
  Argument : guess
```

```
+ CGI : /jsp-examples/error/err.jsp
  Methods : GET
  Argument : name
   Value: audi
  Argument : submit
   Value: Submit


+ CGI : /jsp-examples/sessions/carts.jsp
  Methods : GET
  Argument : item
  Argument : submit
   Value: remove


+ CGI : /jsp-examples/checkbox/checkresult.jsp
  Methods : GET
  Argument : fruit
   Value: melons
  Argument : submit
   Value: Submit


+ CGI : /jsp-examples/colors/colrs.jsp
  Methods : GET,POST
  Argument : action
   Value: Hint
  Argument : color1
  Argument : color2


+ CGI : /jsp-examples/cal/cal1.jsp
  Methods : GET
  Argument : action
   Value: Submit
  Argument : email
  Argument : name


+ CGI : /servlets-examples/servlet/RequestParamExample
  Methods : POST
  Argument : firstname
  Argument : lastname


+ CGI : /servlets-examples/servlet/CookieExample
  Methods : POST
  Argument : cookiename
  Argument : cookievalue


+ CGI : /servlets-examples/servlet/SessionExample;jsessionid=FABCE0CB99995F5261659C8386AA7E47
  Methods : GET,POST
  Argument : dataname
   Value: foo
  Argument : datavalue
   Value: bar
```

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/80/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/80/www

```
The following directories are DAV enabled :
 - /dav/
```

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 7 NetBIOS names have been gathered :

 METASPLOITABLE   = Computer name
 METASPLOITABLE   = Messenger Service
 METASPLOITABLE   = File Server Service
 __MSBROWSE__     = Master Browser
 WORKGROUP        = Workgroup / Domain name
 WORKGROUP        = Master Browser
 WORKGROUP        = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

17219 - phpMyAdmin Detection

Synopsis

The remote web server hosts a database management application written in PHP.

Description

The remote host is running phpMyAdmin, a web-based MySQL administration tool written in PHP.

See Also

https://www.phpmyadmin.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/02/25, Modified: 2022/06/01

Plugin Output

tcp/80/www

```
The following instance of phpMyAdmin was detected on the remote host :

  Version : 3.1.1
  URL     : http://Epic-Metasploitable.epicode/phpMyAdmin/
```

11421 - smtpscan SMTP Fingerprinting

Synopsis

It is possible to fingerprint the remote mail server.

Description

smtpscan is a SMTP fingerprinting tool written by Julien Bordet. It identifies the remote mail server even if the banners were changed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2019/11/22

Plugin Output

tcp/25/smtp

```
This server could be fingerprinted as :

Postfix 2.0.3
Postfix 2.6.5-3 (Ubuntu Karmic)
```