



Kioptrix (1)

Report generated by Tenable Nessus™

Mon, 30 Dec 2024 10:48:47 EST

TABLE OF CONTENTS

Vulnerabilities by Plugin

• 11793 (2) - Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID).....	8
• 11915 (2) - Apache < 1.3.29 Multiple Modules Local Overflow.....	10
• 17746 (2) - OpenSSL 0.9.6 < 0.9.6e Multiple Vulnerabilities.....	12
• 153583 (2) - Apache < 2.4.49 Multiple Vulnerabilities.....	15
• 153584 (2) - Apache < 2.4.49 Multiple Vulnerabilities.....	17
• 158900 (2) - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities.....	19
• 161948 (2) - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities.....	22
• 170113 (2) - Apache 2.4.x < 2.4.55 Multiple Vulnerabilities.....	24
• 171347 (2) - Apache HTTP Server SEoL (<= 1.3.x).....	26
• 172186 (2) - Apache 2.4.x < 2.4.56 Multiple Vulnerabilities.....	28
• 193421 (2) - Apache 2.4.x < 2.4.54 Authentication Bypass.....	30
• 10883 (1) - OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation.....	32
• 11031 (1) - OpenSSH < 3.4 Multiple Remote Overflows.....	34
• 11837 (1) - OpenSSH < 3.7.1 Multiple Vulnerabilities.....	36
• 20007 (1) - SSL Version 2 and 3 Protocol Detection.....	38
• 90022 (1) - OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security Bypass.....	40
• 11030 (2) - Apache Chunked Encoding Remote Overflow.....	42
• 11137 (2) - Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS).....	44
• 12255 (2) - mod_ssl ssl_util_uuencode_binary Remote Overflow.....	47
• 13651 (2) - Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String.....	49
• 17748 (2) - OpenSSL 0.9.6 < 0.9.6k Multiple Vulnerabilities.....	51
• 17751 (2) - OpenSSL 0.9.6 CA Basic Constraints Validation Vulnerability.....	53
• 17752 (2) - OpenSSL < 0.9.7-beta3 Buffer Overflow.....	55
• 31654 (2) - Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow.....	57
• 183391 (2) - Apache 2.4.x < 2.4.58 Multiple Vulnerabilities.....	59
• 192923 (2) - Apache 2.4.x < 2.4.59 Multiple Vulnerabilities.....	61
• 193419 (2) - Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122).....	63

• 193422 (2) - Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability.....	65
• 193423 (2) - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities.....	67
• 193424 (2) - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua).....	69
• 200203 (2) - OpenSSL 0.9.6 < 0.9.6d Vulnerability.....	71
• 10771 (1) - OpenSSH 2.5.x - 2.9 Multiple Vulnerabilities.....	73
• 10823 (1) - OpenSSH < 3.0.2 Multiple Vulnerabilities.....	75
• 10882 (1) - SSH Protocol Version 1 Session Key Retrieval.....	77
• 10954 (1) - OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow.....	79
• 11712 (1) - OpenSSH < 3.6.2 Reverse DNS Lookup Bypass.....	81
• 17702 (1) - OpenSSH < 3.6.1p2 Multiple Vulnerabilities.....	83
• 35291 (1) - SSL Certificate Signed Using Weak Hashing Algorithm.....	85
• 42873 (1) - SSL Medium Strength Cipher Suites Supported (SWEET32).....	87
• 44069 (1) - OpenSSH < 2.9.9p1 Resource Limit Bypass.....	89
• 44072 (1) - OpenSSH < 3.2.3 YP Netgroups Authentication Bypass.....	91
• 44077 (1) - OpenSSH < 4.5 Multiple Vulnerabilities.....	93
• 44078 (1) - OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass.....	95
• 44081 (1) - OpenSSH < 5.7 Multiple Vulnerabilities.....	97
• 73079 (1) - OpenSSH < 6.6 Multiple Vulnerabilities.....	99
• 84638 (1) - OpenSSH < 6.9 Multiple Vulnerabilities.....	101
• 93194 (1) - OpenSSH < 7.3 Multiple Vulnerabilities.....	103
• 96151 (1) - OpenSSH < 7.4 Multiple Vulnerabilities.....	105
• 10816 (2) - Webalizer < 2.01-09 Multiple XSS.....	108
• 11213 (2) - HTTP TRACE / TRACK Methods Allowed.....	110
• 11267 (2) - OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities.....	113
• 12110 (2) - OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS.....	115
• 17696 (2) - Apache HTTP Server 403 Error Page UTF-7 Encoded XSS.....	117
• 17750 (2) - OpenSSL < 0.9.6m / 0.9.7d Denial of Service.....	119
• 17756 (2) - OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability.....	121
• 17759 (2) - OpenSSL < 0.9.8 Weak Default Configuration.....	123

• 17765 (2) - OpenSSL < 0.9.8l Multiple Vulnerabilities.....	125
• 88098 (2) - Apache Server ETag Header Information Disclosure.....	127
• 193420 (2) - Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330).....	129
• 200201 (2) - OpenSSL 0.9.6 < 0.9.6j Multiple Vulnerabilities.....	131
• 200207 (2) - OpenSSL 0.9.6 < 0.9.6i Vulnerability.....	133
• 10802 (1) - OpenSSH < 3.0.1 Multiple Flaws.....	135
• 15901 (1) - SSL Certificate Expiry.....	137
• 26928 (1) - SSL Weak Cipher Suites Supported.....	138
• 31737 (1) - OpenSSH X11 Forwarding Session Hijacking.....	140
• 42880 (1) - SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection.....	142
• 44065 (1) - OpenSSH < 5.2 CBC Plaintext Disclosure.....	144
• 44070 (1) - OpenSSH < 2.9.9p2 echo simulation Information Disclosure.....	146
• 44073 (1) - OpenSSH With OpenPAM DoS.....	148
• 44074 (1) - Portable OpenSSH < 3.8p1 Multiple Vulnerabilities.....	150
• 44076 (1) - OpenSSH < 4.3 scp Command Line Filename Processing Command Injection.....	152
• 44079 (1) - OpenSSH < 4.9 'ForceCommand' Directive Bypass.....	154
• 45411 (1) - SSL Certificate with Wrong Hostname.....	156
• 51192 (1) - SSL Certificate Cannot Be Trusted.....	157
• 51892 (1) - OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Iss.....	159
• 57582 (1) - SSL Self-Signed Certificate.....	161
• 57608 (1) - SMB Signing not required.....	162
• 65821 (1) - SSL RC4 Cipher Suites Supported (Bar Mitzvah).....	164
• 67140 (1) - OpenSSH LoginGraceTime / MaxStartups DoS.....	166
• 81606 (1) - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK).....	168
• 85382 (1) - OpenSSH < 7.0 Multiple Vulnerabilities.....	170
• 89058 (1) - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption).....	172
• 90023 (1) - OpenSSH < 7.2p2 X11Forwarding xauth Command Injection.....	174
• 99359 (1) - OpenSSH < 7.5	176

• 103781 (1) - OpenSSH < 7.6.....	178
• 104743 (1) - TLS Version 1.0 Protocol Detection.....	180
• 159490 (1) - OpenSSH < 7.8.....	182
• 159491 (1) - OpenSSH < 8.0.....	184
• 187201 (1) - OpenSSH < 9.6 Multiple Vulnerabilities.....	186
• 10114 (1) - ICMP Timestamp Request Remote Date Disclosure.....	189
• 19592 (1) - OpenSSH < 4.2 Multiple Vulnerabilities.....	191
• 44075 (1) - OpenSSH < 4.0 known_hosts Plaintext Host Information Disclosure.....	193
• 44080 (1) - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking.....	195
• 53841 (1) - Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Informat.....	197
• 78479 (1) - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE).....	199
• 83738 (1) - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam).....	201
• 83875 (1) - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam).....	203
• 11219 (6) - Nessus SYN scanner.....	205
• 11111 (4) - RPC Services Enumeration.....	207
• 22964 (4) - Service Detection.....	209
• 10107 (2) - HTTP Server Type and Version.....	210
• 11422 (2) - Web Server Unconfigured - Default Install Page Present.....	211
• 24260 (2) - HyperText Transfer Protocol (HTTP) Information.....	212
• 43111 (2) - HTTP Methods Allowed (per directory).....	215
• 48204 (2) - Apache HTTP Server Version.....	217
• 57323 (2) - OpenSSL Version Detection.....	219
• 10150 (1) - Windows NetBIOS / SMB Remote Host Information Disclosure.....	220
• 10223 (1) - RPC portmapper Service Detection.....	221
• 10267 (1) - SSH Server Type and Version Information.....	222
• 10287 (1) - Traceroute Information.....	223
• 10863 (1) - SSL Certificate Information.....	224
• 10881 (1) - SSH Protocol Versions Supported.....	226
• 11011 (1) - Microsoft Windows SMB Service Detection.....	227

• 11936 (1) - OS Identification.....	228
• 19506 (1) - Nessus Scan Information.....	229
• 21643 (1) - SSL Cipher Suites Supported.....	231
• 25220 (1) - TCP/IP Timestamps Supported.....	233
• 35716 (1) - Ethernet Card Manufacturer Detection.....	234
• 45410 (1) - SSL Certificate 'commonName' Mismatch.....	235
• 45590 (1) - Common Platform Enumeration (CPE).....	236
• 51891 (1) - SSL Session Resume Supported.....	237
• 53335 (1) - RPC portmapper (TCP).....	238
• 53360 (1) - SSL Server Accepts Weak Diffie-Hellman Keys.....	239
• 54615 (1) - Device Type.....	240
• 56984 (1) - SSL / TLS Versions Supported.....	241
• 57041 (1) - SSL Perfect Forward Secrecy Cipher Suites Supported.....	242
• 58768 (1) - SSL Resume With Different Cipher Issue.....	244
• 66334 (1) - Patch Report.....	245
• 70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported.....	247
• 84502 (1) - HSTS Missing From HTTPS Server.....	249
• 86420 (1) - Ethernet MAC Addresses.....	250
• 94761 (1) - SSL Root Certification Authority Certificate Information.....	251
• 106716 (1) - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check).....	252
• 110723 (1) - Target Credential Status by Authentication Protocol - No Credentials Provided.....	253
• 117886 (1) - OS Security Patch Assessment Not Available.....	255
• 135860 (1) - WMI Not Available.....	256
• 149334 (1) - SSH Password Authentication Accepted.....	257
• 156899 (1) - SSL/TLS Recommended Cipher Suites.....	258
• 181418 (1) - OpenSSH Detection.....	260

Vulnerabilities by Plugin

11793 (2) - Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The remote host appears to be running a version of Apache which is older than 1.3.28

There are several flaws in this version, including a denial of service in redirect handling, a denial of service with control character handling in the 'rotatelogs' utility and a file descriptor leak in third-party module handling.

*** Note that Nessus solely relied on the version number

*** of the remote server to issue this warning. This might

*** be a false positive

See Also

<http://www.apache.org/dist/httpd/Announcement.html>

Solution

Upgrade to version 1.3.28

Risk Factor

High

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

0.5085

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 8226
CVE CVE-2003-0460

Plugin Information

Published: 2003/07/18, Modified: 2018/06/29

Plugin Output

10.0.2.4 (tcp/80/www)

```
Version source      : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version   : 1.3.20
Fixed version       : 1.3.28
```

10.0.2.4 (tcp/443/www)

```
Version source      : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version   : 1.3.20
Fixed version       : 1.3.28
```

11915 (2) - Apache < 1.3.29 Multiple Modules Local Overflow

Synopsis

The remote web server is affected by multiple local buffer overflow vulnerabilities.

Description

The remote host appears to be running a version of the Apache web server which is older than 1.3.29. Such versions are reportedly affected by local buffer overflow vulnerabilities in the mod_alias and mod_rewrite modules. An attacker could exploit these vulnerabilities to execute arbitrary code in the context of the affected application.

*** Note that Nessus solely relied on the version number
*** of the remote server to issue this warning. This might
*** be a false positive

See Also

<https://www.securityfocus.com/archive/1/342674/30/0/threaded>

Solution

Upgrade to Apache web server version 1.3.29 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

0.0008

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

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

References

BID	8911
CVE	CVE-2003-0542
XREF	Secunia:10096
XREF	Secunia:10845
XREF	Secunia:17311
XREF	CWE:119

Plugin Information

Published: 2003/11/01, Modified: 2018/11/15

Plugin Output

10.0.2.4 (tcp/80/www)

```
Version source      : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version   : 1.3.20
Fixed version       : 1.3.29
```

10.0.2.4 (tcp/443/www)

```
Version source      : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version   : 1.3.20
Fixed version       : 1.3.29
```

17746 (2) - OpenSSL 0.9.6 < 0.9.6e Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.6e. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.6e advisory.

- The ASN1 library in OpenSSL 0.9.6d and earlier, and 0.9.7-beta2 and earlier, allows remote attackers to cause a denial of service via invalid encodings. (CVE-2002-0659)

- Buffer overflows in OpenSSL 0.9.6d and earlier, and 0.9.7-beta2 and earlier, allow remote attackers to execute arbitrary code via (1) a large client master key in SSL2 or (2) a large session ID in SSL3. (CVE-2002-0656)

- OpenSSL 0.9.6d and earlier, and 0.9.7-beta2 and earlier, does not properly handle ASCII representations of integers on 64 bit platforms, which could allow attackers to cause a denial of service and possibly execute arbitrary code. (CVE-2002-0655)

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.cve.org/CVERecord?id=CVE-2002-0655>
<https://www.cve.org/CVERecord?id=CVE-2002-0656>
<https://www.cve.org/CVERecord?id=CVE-2002-0659>
<https://www.openssl.org/news/secadv/20020730.txt>

Solution

Upgrade to OpenSSL version 0.9.6e 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

7.0

EPSS Score

0.7302

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	5362
BID	5363
BID	5364
BID	5366
CVE	CVE-2002-0655
CVE	CVE-2002-0656
CVE	CVE-2002-0659
XREF	CERT-CC:CA-2002-23
XREF	CERT:102795
XREF	CERT:308891

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2012/01/04, Modified: 2024/10/23

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.6e
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.6e
```

10.0.2.4 (tcp/443/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.6e
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.6e
```

153583 (2) - 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 chosen 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

0.9668

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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/  
Installed version : 1.3.20  
Fixed version  : 2.4.49
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/  
Installed version : 1.3.20  
Fixed version  : 2.4.49
```


153584 (2) - 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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.49
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.49
```

158900 (2) - 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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.53
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/
```

```
Installed version : 1.3.20  
Fixed version    : 2.4.53
```

161948 (2) - 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_lua's 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

0.0104

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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.54
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.54
```

170113 (2) - 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

0.0329

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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/  
Installed version : 1.3.20  
Fixed version  : 2.4.55
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/  
Installed version : 1.3.20  
Fixed version  : 2.4.55
```

171347 (2) - Apache HTTP Server SEoL (<= 1.3.x)

Synopsis

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

Description

According to its version, Apache HTTP Server is less than or equal to 1.3.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

<http://archive.apache.org/dist/httpd/Announcement1.3.html>

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/I:C/A:C)

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/80/www)

```
URL : http://10.0.2.4/
Installed version : 1.3.20
Security End of Life : February 2, 2010
Time since Security End of Life (Est.) : >= 14 years
```

10.0.2.4 (tcp/443/www)

```
URL : https://10.0.2.4/
Installed version : 1.3.20
Security End of Life : February 2, 2010
Time since Security End of Life (Est.) : >= 14 years
```

172186 (2) - 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

0.0117

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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.56
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.56
```

193421 (2) - 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

0.0074

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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.54
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.54
```

10883 (1) - OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation

Synopsis

Arbitrary code may be run on the remote host.

Description

You are running a version of OpenSSH which is older than 3.1.

Versions prior than 3.1 are vulnerable to an off by one error that allows local users to gain root access, and it may be possible for remote users to similarly compromise the daemon for remote access.

In addition, a vulnerable SSH client may be compromised by connecting to a malicious SSH daemon that exploits this vulnerability in the client code, thus compromising the client system.

Solution

Upgrade to OpenSSH 3.1 or apply the patch for prior versions. (See: <http://www.openssh.org>)

Risk Factor

Critical

VPR Score

8.4

EPSS Score

0.0177

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	4241
CVE	CVE-2002-0083
XREF	CWE:189

Exploitable With

Core Impact (true)

Plugin Information

Published: 2002/03/07, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 3.1p1
```

11031 (1) - OpenSSH < 3.4 Multiple Remote Overflows

Synopsis

The remote host has an application that is affected multiple vulnerabilities.

Description

According to its banner, the remote host appears to be running OpenSSH version 3.4 or older. Such versions are reportedly affected by multiple flaws. An attacker may exploit these vulnerabilities to gain a shell on the remote system.

Note that several distributions patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :

`rpm -q openssh-server` Returns :

`openssh-server-3.1p1-6`

See Also

<http://www.openssh.com/txt/preauth.adv>

Solution

Upgrade to OpenSSH 3.4 or contact your vendor for a patch.

Risk Factor

Critical

VPR Score

6.7

EPSS Score

0.7197

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

BID	5093
CVE	CVE-2002-0639
CVE	CVE-2002-0640

Plugin Information

Published: 2002/06/25, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 3.4
```

11837 (1) - OpenSSH < 3.7.1 Multiple Vulnerabilities

Synopsis

The remote SSH service is affected by various memory bugs.

Description

According to its banner, the remote SSH server is running a version of OpenSSH older than 3.7.1. Such versions are vulnerable to a flaw in the buffer management functions that might allow an attacker to execute arbitrary commands on this host.

An exploit for this issue is rumored to exist.

Note that several distributions patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :

```
rpm -q openssh-server
```

returns :

```
openssh-server-3.1p1-13 (RedHat 7.x) openssh-server-3.4p1-7 (RedHat 8.0) openssh-server-3.5p1-11 (RedHat 9)
```

See Also

<https://marc.info/?l=openbsd-misc&m=106375452423794&w=2>

<https://marc.info/?l=openbsd-misc&m=106375456923804&w=2>

Solution

Upgrade to OpenSSH 3.7.1 or later.

Risk Factor

Critical

VPR Score

5.5

EPSS Score

0.7142

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	8628
CVE	CVE-2003-0682
CVE	CVE-2003-0693
CVE	CVE-2003-0695
CVE	CVE-2004-2760
XREF	RHSA:2003:279
XREF	SuSE:SUSE-SA:2003:039
XREF	CWE:16

Plugin Information

Published: 2003/09/16, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 3.7.1
```

20007 (1) - SSL Version 2 and 3 Protocol Detection

Synopsis

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

Description

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

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

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

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

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

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?b06c7e95>

<http://www.nessus.org/u?247c4540>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<http://www.nessus.org/u?5d15ba70>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

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:I/C/A:C)

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/443/www)

- SSLv2 is enabled and the server supports at least one cipher.

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	---	-----	---
EXP-RC2-CBC-MD5 export		RSA (512)	RSA	RC2-CBC (40)	MD5
EXP-RC4-MD5 export		RSA (512)	RSA	RC4 (40)	MD5

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	---	-----	---
DES-CBC3-MD5		RSA	RSA	3DES-CBC (168)	MD5

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	---	-----	---
RC4-MD5		RSA	RSA	RC4 (128)	MD5

The fields above are :

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

- SSLv3 is enabled and the server supports at least one cipher.

Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	---	-----	---
EXP-EDH-RSA-DES-CBC-SHA SHA1 export		DH (512)	RSA	DES-CBC (40)	
EDH-RSA-DES-CBC-SHA		DH	RSA	DES-CBC (56)	SHA
[...]					

90022 (1) - 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

0.0079

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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 7.2
```

11030 (2) - Apache Chunked Encoding Remote Overflow

Synopsis

The remote web server is vulnerable to a remote code execution attack.

Description

The remote Apache web server is affected by the Apache web server chunk handling vulnerability.

If safe checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched Apache versions 1.2.2 and above, 1.3 through 1.3.24, and 2.0 through 2.0.36 are affected, the remote server may be running a patched version of Apache.

See Also

http://httpd.apache.org/info/security_bulletin_20020617.txt

http://httpd.apache.org/info/security_bulletin_20020620.txt

Solution

Upgrade to Apache web server version 1.3.26 / 2.0.39 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

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

VPR Score

5.9

EPSS Score

0.7873

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	5033
CVE	CVE-2002-0392

Exploitable With

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

Plugin Information

Published: 2002/06/17, Modified: 2020/06/12

Plugin Output

10.0.2.4 (tcp/80/www)
10.0.2.4 (tcp/443/www)

11137 (2) - Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The remote host is running a version of Apache web server prior to 1.3.27. It is, therefore, affected by multiple vulnerabilities :

- There is a cross-site scripting vulnerability caused by a failure to filter HTTP/1.1 'Host' headers that are sent by browsers.
- A vulnerability in the handling of the Apache scorecard could allow an attacker to cause a denial of service.
- A buffer overflow vulnerability exists in the 'support/ab.c' read_connection() function. The ab.c file is a benchmarking support utility that is provided with the Apache web server.

See Also

<https://seclists.org/bugtraq/2002/Oct/199>
<http://www.nessus.org/u?767573c2>
<https://seclists.org/bugtraq/2002/Nov/163>
<http://www.nessus.org/u?e06ce83b>

Solution

Upgrade to Apache web server version 1.3.27 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

6.0

EPSS Score

0.967

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	5847
BID	5884
BID	5887
BID	5995
BID	5996
CVE	CVE-2002-0839
CVE	CVE-2002-0840
CVE	CVE-2002-0843
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: 2002/10/04, Modified: 2018/11/15

Plugin Output

10.0.2.4 (tcp/80/www)

```
Version source      : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version   : 1.3.20
Fixed version       : 1.3.27
```

10.0.2.4 (tcp/443/www)

```
Version source      : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version   : 1.3.20
Fixed version       : 1.3.27
```

12255 (2) - mod_ssl ssl_util_uencode_binary Remote Overflow

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote host is using a version of mod_ssl that is older than 2.8.18.

This version is vulnerable to a flaw that could allow an attacker to disable the remote website remotely, or to execute arbitrary code on the remote host.

Note that several Linux distributions patched the old version of this module. Therefore, this alert might be a false-positive. Please check with your vendor to determine if you really are vulnerable to this flaw.

Solution

Upgrade to version 2.8.18 (Apache 1.3) or to Apache 2.0.50.

Risk Factor

High

VPR Score

5.5

EPSS Score

0.5036

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	10355
CVE	CVE-2004-0488

Plugin Information

Published: 2004/05/29, Modified: 2018/07/14

Plugin Output

10.0.2.4 (tcp/80/www)

10.0.2.4 (tcp/443/www)

13651 (2) - Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String

Synopsis

The remote web server is using a module that is affected by a remote code execution vulnerability.

Description

The remote host is using a version vulnerable of mod_ssl which is older than 2.8.19. There is a format string condition in the log functions of the remote module which may allow an attacker to execute arbitrary code on the remote host.

*** Some vendors patched older versions of mod_ssl, so this
*** might be a false positive. Check with your vendor to determine
*** if you have a version of mod_ssl that is patched for this
*** vulnerability

See Also

<http://marc.info/?l=apache-modssl&m=109001100906749&w=2>

<https://marc.info/?l=bugtraq&m=109005001205991&w=2>

Solution

Upgrade to mod_ssl version 2.8.19 or newer

Risk Factor

High

VPR Score

5.3

EPSS Score

0.9092

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	10736
CVE	CVE-2004-0700

Plugin Information

Published: 2004/07/16, Modified: 2020/12/22

Plugin Output

10.0.2.4 (tcp/80/www)
10.0.2.4 (tcp/443/www)

17748 (2) - OpenSSL 0.9.6 < 0.9.6k Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.6k. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.6k advisory.

- OpenSSL 0.9.6 and 0.9.7 does not properly track the number of characters in certain ASN.1 inputs, which allows remote attackers to cause a denial of service (crash) via an SSL client certificate that causes OpenSSL to read past the end of a buffer when the long form is used. (CVE-2003-0544)

- Integer overflow in OpenSSL 0.9.6 and 0.9.7 allows remote attackers to cause a denial of service (crash) via an SSL client certificate with certain ASN.1 tag values. (CVE-2003-0543)

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.cve.org/CVERecord?id=CVE-2003-0543>

<https://www.cve.org/CVERecord?id=CVE-2003-0544>

<https://www.openssl.org/news/secadv/20030930.txt>

Solution

Upgrade to OpenSSL version 0.9.6k 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

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

VPR Score

4.4

EPSS Score

0.9196

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	8732
CVE	CVE-2003-0543
CVE	CVE-2003-0544
XREF	CERT-CC:CA-2003-26
XREF	CERT:255484
XREF	CERT:380864

Plugin Information

Published: 2012/01/04, Modified: 2024/10/23

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.6k
```

10.0.2.4 (tcp/443/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.6k
```

17751 (2) - OpenSSL 0.9.6 CA Basic Constraints Validation Vulnerability

Synopsis

The remote server is affected by a certificate validation vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7.

Such versions do not verify the Basic Constraint for some certificates. A remote attacker could perform a man-in-the-middle attack.

Details on this weakness are missing. It is related to CVE-2002-0970. OpenSSL 0.9.6 was reported as 'probably' vulnerable.

See Also

<http://www.nessus.org/u?8e41b7c3>

Solution

Upgrade to OpenSSL 0.9.7 or later.

Risk Factor

High

VPR Score

6.6

EPSS Score

0.0026

CVSS v2.0 Base Score

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

References

CVE CVE-2009-0653

XREF CWE:287

Plugin Information

Published: 2012/01/04, Modified: 2024/10/23

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.7
```

10.0.2.4 (tcp/443/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.7
```

17752 (2) - OpenSSL < 0.9.7-beta3 Buffer Overflow

Synopsis

The remote server is affected by an arbitrary code execution vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7-beta3.

If Kerberos is enabled, a remote attacker could trigger a buffer overflow with a long master key and execute arbitrary code.

Solution

Upgrade to OpenSSL 0.9.7 or later.

Risk Factor

High

VPR Score

5.8

EPSS Score

0.0209

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	5361
CVE	CVE-2002-0657
XREF	CERT-CC:CA-2002-23
XREF	CERT:561275

Plugin Information

Published: 2012/01/04, Modified: 2024/10/07

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.7-beta3
```

10.0.2.4 (tcp/443/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.7-beta3
```


31654 (2) - Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow

Synopsis

The remote version of Apache is vulnerable to an off-by-one buffer overflow attack.

Description

The remote host appears to be running a version of Apache which is older than 1.3.37.

This version contains an off-by-one buffer overflow in the mod_rewrite module.

See Also

<https://seclists.org/fulldisclosure/2006/Jul/671>

<https://www.securityfocus.com/archive//443870>

Solution

Upgrade to version 1.3.37 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

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

VPR Score

4.9

EPSS Score

0.9352

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	19204
CVE	CVE-2006-3747
XREF	EDB-ID:3680
XREF	CWE:189

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2008/03/26, Modified: 2018/11/15

Plugin Output

10.0.2.4 (tcp/80/www)

```
Version source      : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version   : 1.3.20
Fixed version       : 1.3.37
```

10.0.2.4 (tcp/443/www)

```
Version source      : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version   : 1.3.20
Fixed version       : 1.3.37
```

183391 (2) - 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 where 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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.58
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.58
```

192923 (2) - 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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.59
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.59
```

193419 (2) - 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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/  
Installed version : 1.3.20  
Fixed version  : 2.4.58
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/  
Installed version : 1.3.20  
Fixed version  : 2.4.58
```


193422 (2) - 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: Richter 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

0.0032

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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/  
Installed version : 1.3.20  
Fixed version  : 2.4.54
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/  
Installed version : 1.3.20  
Fixed version  : 2.4.54
```

193423 (2) - 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

0.1724

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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.54
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.54
```

193424 (2) - 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

0.0223

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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.54
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/
Installed version : 1.3.20
Fixed version  : 2.4.54
```

200203 (2) - OpenSSL 0.9.6 < 0.9.6d Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.6d. It is, therefore, affected by a vulnerability as referenced in the 0.9.6d advisory.

- OpenSSL 0.9.6 before 0.9.6d does not properly handle unknown message types, which allows remote attackers to cause a denial of service (infinite loop), as demonstrated using the Codenomicon TLS Test Tool. (CVE-2004-0081)

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.cve.org/CVERecord?id=CVE-2004-0081>

<https://www.openssl.org/news/secadv/20030317.txt>

Solution

Upgrade to OpenSSL version 0.9.6d 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

4.4

EPSS Score

0.0038

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-2004-0081

Plugin Information

Published: 2024/06/07, Modified: 2024/10/07

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner          : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.6d
```

10.0.2.4 (tcp/443/www)

```
Banner          : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.6d
```


10771 (1) - OpenSSH 2.5.x - 2.9 Multiple Vulnerabilities

Synopsis

The remote version of OpenSSH contains multiple vulnerabilities.

Description

According to its banner, the remote host appears to be running OpenSSH version between 2.5.x and 2.9. Such versions reportedly contain multiple vulnerabilities :

- sftp-server does not respect the 'command=' argument of keys in the authorized_keys2 file. (CVE-2001-0816)

- sshd does not properly handle the 'from=' argument of keys in the authorized_keys2 file. If a key of one type (e.g. RSA) is followed by a key of another type (e.g. DSA) then the options for the latter will be applied to the former, including 'from=' restrictions. This problem allows users to circumvent the system policy and login from disallowed source IP addresses. (CVE-2001-1380)

See Also

http://www.openbsd.org/advisories/ssh_option.txt

<http://www.nessus.org/u?759da6a7>

<http://www.openssh.com/txt/release-2.9.9>

Solution

Upgrade to OpenSSH 2.9.9

Risk Factor

High

VPR Score

5.3

EPSS Score

0.0467

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	3345
BID	3369
CVE	CVE-2001-0816
CVE	CVE-2001-1380
XREF	CERT:905795

Plugin Information

Published: 2001/09/28, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 2.9.9
```

10823 (1) - OpenSSH < 3.0.2 Multiple Vulnerabilities

Synopsis

The SSH service running on the remote host has multiple vulnerabilities.

Description

You are running a version of OpenSSH which is older than 3.0.2.

Versions prior than 3.0.2 have the following vulnerabilities :

- When the UseLogin feature is enabled, a local user could export environment variables, resulting in command execution as root. The UseLogin feature is disabled by default. (CVE-2001-0872)

- A local information disclosure vulnerability.

Only FreeBSD hosts are affected by this issue.

(CVE-2001-1029)

See Also

<https://seclists.org/bugtraq/2001/Sep/208>

<https://www.freebsd.org/releases/4.4R/errata.html>

<http://www.nessus.org/u?f85ed76c>

Solution

Upgrade to OpenSSH 3.0.2 or apply the patch for prior versions. (Available at: <ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH>)

Risk Factor

High

VPR Score

6.7

EPSS Score

0.0099

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	3614
CVE	CVE-2001-0872
CVE	CVE-2001-1029

Plugin Information

Published: 2001/12/10, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 3.0.2
```

10882 (1) - SSH Protocol Version 1 Session Key Retrieval

Synopsis

The remote service offers an insecure cryptographic protocol.

Description

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Solution

Disable compatibility with version 1 of the SSH protocol.

Risk Factor

High

CVSS v3.0 Base Score

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

VPR Score

6.3

EPSS Score

0.0161

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	2344
CVE	CVE-2001-0361
CVE	CVE-2001-0572
CVE	CVE-2001-1473
XREF	CWE:310

Plugin Information

Published: 2002/03/06, Modified: 2023/10/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

10954 (1) - OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow

Synopsis

Arbitrary code may be run on the remote host.

Description

You are running a version of OpenSSH older than OpenSSH 3.2.1.

A buffer overflow exists in the daemon if AFS is enabled on your system, or if the options `KerberosTgtPassing` or `AFSTokenPassing` are enabled. Even in this scenario, the vulnerability may be avoided by enabling `UsePrivilegeSeparation`.

Versions prior to 2.9.9 are vulnerable to a remote root exploit. Versions prior to 3.2.1 are vulnerable to a local root exploit.

Solution

Upgrade to version 3.2.1 or later.

Risk Factor

High

VPR Score

6.3

EPSS Score

0.0004

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	4560
CVE	CVE-2002-0575

Plugin Information

Published: 2002/05/12, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 3.2.1
```


11712 (1) - OpenSSH < 3.6.2 Reverse DNS Lookup Bypass

Synopsis

The remote host has an application that is affected by DNS lookup bypass vulnerability.

Description

According to its banner, the remote host appears to be running OpenSSH-portable version 3.6.1 or older.

There is a flaw in such version that could allow an attacker to bypass the access controls set by the administrator of this server.

OpenSSH features a mechanism that can restrict the list of hosts a given user can log from by specifying a pattern in the user key file (ie: *.mynetwork.com would let a user connect only from the local network).

However there is a flaw in the way OpenSSH does reverse DNS lookups.

If an attacker configures a DNS server to send a numeric IP address when a reverse lookup is performed, this mechanism could be circumvented.

Solution

Upgrade to OpenSSH 3.6.2 or later.

Risk Factor

High

VPR Score

5.5

EPSS Score

0.1506

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	7831
CVE	CVE-2003-0386
XREF	CERT:978316

Plugin Information

Published: 2003/06/10, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 3.6.2
```

17702 (1) - OpenSSH < 3.6.1p2 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 earlier than 3.6.1p2. When compiled for the AIX operating system with a compiler other than that of the native AIX compiler, an error exists that can allow dynamic libraries in the current directory to be loaded before dynamic libraries in the system paths. This behavior can allow local users to escalate privileges by creating, loading and executing their own malicious replacement libraries.

See Also

<https://www.openssh.com/txt/release-3.6.1p2>

<https://www.securityfocus.com/archive/1/320038/2003-04-25/2003-05-01/0>

Solution

Upgrade to OpenSSH 3.6.1p2 or later.

Risk Factor

High

VPR Score

7.4

EPSS Score

0.0052

CVSS v2.0 Base Score

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

References

CVE CVE-2002-0746

Plugin Information

Published: 2011/11/18, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2  
Installed version   : 2.9p2  
Fixed version       : 3.6.1p2
```

35291 (1) - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

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

Description

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

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

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

See Also

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

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

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

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

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

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

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.2

EPSS Score

0.0729

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/443/www)

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

```
Subject          : C=-/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
Signature Algorithm : MD5 With RSA Encryption
Valid From       : Sep 26 09:32:06 2009 GMT
Valid To        : Sep 26 09:32:06 2010 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDDCCA3WgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBuzELMAkGA1UEBhMCLs0xEjAQBgNVBAGTCVNVbWVtdGF0ZTERMA8GA1UEBxMIU29tZUNpdG
+fHHn+CjU1DX44LPDNOWwOl6Uqb+GtZJv6juVetDwcTbbocC2BM+6x6gyV/H6aYuCssCwrOuVKWp719xVpadjITUmhh
+uB81qyqopt//
Z4THww7SezLJQXi1+Grmp3iFDAGMBAAGjggEcMIIBGDADBgNVHQ4EFgQU70dRS0NrbNB8gE9qUjcw8LF8xKAwegGA1UdIwSB4DCB3YAU70dRS0Nrb
+jDQzA6Cu7ntxjrlXxEjHFBbBf4iEMJDnuQTFGvICQIcrqJoH3lqAO73u4TeBDjhv5n+h
+S37CHd1lvRgoOay9dWaLKQyUThgKF2HcPwMZIj2froo5eihM=
-----END CERTIFICATE-----
```

42873 (1) - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

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

Description

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

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

See Also

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

<https://sweet32.info>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.1

EPSS Score

0.0398

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/443/www)

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
DES-CBC3-MD5	0x07, 0x00, 0xC0	RSA	RSA	3DES-CBC (168)	MD5
EDH-RSA-DES-CBC3-SHA	0x00, 0x16	DH	RSA	3DES-CBC (168)	
SHA1					
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	
SHA1					

The fields above are :

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

44069 (1) - OpenSSH < 2.9.9p1 Resource Limit Bypass

Synopsis

The remote SSH service is affected by a denial of service vulnerability.

Description

According to its banner, the remote host is running a version of OpenSSH earlier than 2.9.9/2.9.9p1. Such versions fail to initiate a Pluggable Authentication Module (PAM) session if commands are executed with no pty. A remote, unauthenticated attacker, exploiting this flaw, could bypass resource limits (rlimits) set in pam.d.

See Also

<https://marc.info/?l=bugtraq&m=99324968918628&w=2>

Solution

Upgrade to OpenSSH 2.9.9/2.9.9p1 or later.

Risk Factor

High

VPR Score

5.2

EPSS Score

0.0017

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	2917
CVE	CVE-2001-1459
XREF	CERT:797027

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 2.9.9p1 / 2.9.9
```

44072 (1) - OpenSSH < 3.2.3 YP Netgroups Authentication Bypass

Synopsis

The remote SSH server has an authentication bypass vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is older than 3.2.3. It therefore may be affected by an authentication bypass issue. On systems using YP with netgroups, sshd authenticates users via ACL by checking for the requested username and password. Under certain conditions when doing ACL checks, it may instead use the password entry of a different user for authentication. This means unauthorized users could authenticate successfully, and authorized users could be locked out.

See Also

<http://monkey.org/openbsd/archive/bugs/0205/msg00141.html>

<https://www.openssh.com/txt/release-3.2.3>

<http://www.openbsd.org/errata31.html#sshbsdauth>

Solution

Upgrade to OpenSSH 3.2.3 or later.

Risk Factor

High

VPR Score

5.2

EPSS Score

0.004

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 4803
CVE CVE-2002-0765

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 3.2.3
```

44077 (1) - OpenSSH < 4.5 Multiple Vulnerabilities

Synopsis

The remote SSH service is affected by multiple vulnerabilities.

Description

According to its banner, the remote host is running a version of OpenSSH prior to 4.5. Versions before 4.5 are affected by the following vulnerabilities :

- A client-side NULL pointer dereference, caused by a protocol error from a malicious server, which could cause the client to crash. (CVE-2006-4925)
- A privilege separation vulnerability exists, which could allow attackers to bypass authentication. The vulnerability is caused by a design error between privileged processes and their child processes. Note that this particular issue is only exploitable when other vulnerabilities are present. (CVE-2006-5794)
- An attacker that connects to the service before it has finished creating keys could force the keys to be recreated. This could result in a denial of service for any processes that relies on a trust relationship with the server. Note that this particular issue only affects the Apple implementation of OpenSSH on Mac OS X. (CVE-2007-0726)

See Also

<https://www.openssh.com/txt/release-4.5>

https://support.apple.com/kb/TA24626?locale=en_US

<https://www.openssh.com/security.html>

Solution

Upgrade to OpenSSH 4.5 or later.

For Mac OS X 10.3, apply Security Update 2007-003.

For Mac OS X 10.4, upgrade to 10.4.9.

Risk Factor

High

VPR Score

5.5

EPSS Score

0.0444

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	20956
CVE	CVE-2006-4925
CVE	CVE-2006-5794
CVE	CVE-2007-0726

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 4.5
```

44078 (1) - OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass

Synopsis

Remote attackers may be able to bypass authentication.

Description

According to the banner, OpenSSH earlier than 4.7 is running on the remote host. Such versions contain an authentication bypass vulnerability. In the event that OpenSSH cannot create an untrusted cookie for X, for example due to the temporary partition being full, it will use a trusted cookie instead. This allows attackers to violate intended policy and gain privileges by causing their X client to be treated as trusted.

See Also

<http://www.openssh.com/txt/release-4.7>

Solution

Upgrade to OpenSSH 4.7 or later.

Risk Factor

High

VPR Score

5.3

EPSS Score

0.014

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	25628
CVE	CVE-2007-4752
CVE	CVE-2007-2243
XREF	CWE:20

XREF

CWE:287

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 4.7
```


44081 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 5.7
```

73079 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 6.6
```

84638 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2  
Installed version   : 2.9p2  
Fixed version       : 6.9
```

93194 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 7.3
```


96151 (1) - 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

0.1278

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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2  
Installed version   : 2.9p2  
Fixed version       : 7.4
```

10816 (2) - Webalizer < 2.01-09 Multiple XSS

Synopsis

A web application on the remote host has multiple cross-site scripting vulnerabilities.

Description

Webalizer, a web server log analysis application, was detected on the remote host. This version of Webalizer has multiple cross-site scripting vulnerabilities that could allow malicious HTML tags to be injected in the reports.

See Also

<https://seclists.org/bugtraq/2001/Oct/223>

Solution

Upgrade to Version 2.01-09 and change the directory in 'OutputDir'.

Risk Factor

Medium

VPR Score

5.9

EPSS Score

0.0169

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	3473
CVE	CVE-2001-0835
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: 2001/12/03, Modified: 2021/01/19

Plugin Output

10.0.2.4 (tcp/80/www)
10.0.2.4 (tcp/443/www)

11213 (2) - 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

10.0.2.4 (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 /Nessus599703965.html HTTP/1.1
Connection: Close
Host: 10.0.2.4
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

----- snip ----- \n\nand received the
following response from the remote server : \n\n----- snip
-----\nHTTP/1.1 200 OK
Date: Mon, 30 Dec 2024 20:43:27 GMT
Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE /Nessus599703965.html HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: iso-8859-1,*,utf-8
Accept-Language: en
Connection: Close
Host: 10.0.2.4
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

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

10.0.2.4 (tcp/443/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 /Nessus1628421461.html HTTP/1.1

```
Connection: Close
Host: 10.0.2.4
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

----- snip -----\n\nand received the
following response from the remote server : \n\n----- snip
-----\nHTTP/1.1 200 OK

```
Date: Mon, 30 Dec 2024 20:43:27 GMT
Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE /Nessus1628421461.html HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: iso-8859-1,*,utf-8
Accept-Language: en
Connection: Close
Host: 10.0.2.4
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

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


11267 (2) - OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities

Synopsis

The remote host has an application that is affected by multiple vulnerabilities.

Description

According to its banner, the remote host is using a version of OpenSSL older than 0.9.6j or 0.9.7b.

This version is vulnerable to a timing-based attack that could allow an attacker to guess the content of fixed data blocks and may eventually be able to guess the value of the private RSA key of the server.

An attacker may use this implementation flaw to sniff the data going to this host and decrypt some parts of it, as well as impersonate the server and perform man-in-the-middle attacks.

See Also

<https://www.openssl.org/news/secadv/20030219.txt>

<http://eprint.iacr.org/2003/052/>

Solution

Upgrade to version 0.9.6j (0.9.7b) or newer.

Risk Factor

Medium

VPR Score

5.1

EPSS Score

0.2346

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 6884

BID	7148
CVE	CVE-2003-0078
CVE	CVE-2003-0131
CVE	CVE-2003-0147
XREF	RHSA:2003:101-01
XREF	SuSE:SUSE-SA:2003:024

Plugin Information

Published: 2003/02/20, Modified: 2022/04/11

Plugin Output

10.0.2.4 (tcp/80/www)
10.0.2.4 (tcp/443/www)

12110 (2) - OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS

Synopsis

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

Description

According to its banner, the remote host is using a version of OpenSSL which is older than 0.9.6m / 0.9.7d. There are several bugs in such versions that may allow an attacker to cause a denial of service against the remote host.

See Also

<https://www.openssl.org/news/secadv/20040317.txt>

<https://seclists.org/bugtraq/2004/Mar/155>

Solution

Upgrade to version 0.9.6m / 0.9.7d or newer.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.0065

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	9899
CVE	CVE-2004-0079
CVE	CVE-2004-0081
CVE	CVE-2004-0112

Plugin Information

Published: 2004/03/17, Modified: 2018/11/15

Plugin Output

10.0.2.4 (tcp/80/www)

10.0.2.4 (tcp/443/www)

17696 (2) - Apache HTTP Server 403 Error Page UTF-7 Encoded XSS

Synopsis

The web server running on the remote host has a cross-site scripting vulnerability.

Description

According to its banner, the version of Apache HTTP Server running on the remote host can be used in cross-site scripting (XSS) attacks. Making a specially crafted request can inject UTF-7 encoded script code into a 403 response page, resulting in XSS attacks.

This is actually a web browser vulnerability that occurs due to non-compliance with RFC 2616 (refer to BID 29112). Apache HTTP Server is not vulnerable, but its default configuration can trigger the non-compliant, exploitable behavior in vulnerable browsers.

See Also

<https://seclists.org/bugtraq/2008/May/109>

<https://seclists.org/bugtraq/2008/May/166>

Solution

Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions use a default configuration setting that prevents exploitation in vulnerable web browsers.

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

3.3

EPSS Score

0.1236

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

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

References

BID	29112
CVE	CVE-2008-2168
XREF	CWE:79

Plugin Information

Published: 2011/11/18, Modified: 2018/11/15

Plugin Output

10.0.2.4 (tcp/80/www)

```
Version source   : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version    : 1.3.41
```

10.0.2.4 (tcp/443/www)

```
Version source   : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version    : 1.3.41
```

17750 (2) - OpenSSL < 0.9.6m / 0.9.7d Denial of Service

Synopsis

The remote server is vulnerable to a denial of service attack.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6m or 0.9.7d.

A remote attacker can crash the server by sending an overly long Kerberos ticket or a crafted SSL/TLS handshake.

See Also

<https://www.us-cert.gov/ncas/alerts/ta04-078a>

<https://www.openssl.org/news/secadv/20040317.txt>

<http://marc.info/?l=bugtraq&m=107953412903636&w=2>

Solution

Upgrade to OpenSSL 0.9.6m / 0.9.7d or later.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.0065

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 9899

CVE CVE-2004-0079
CVE CVE-2004-0112
XREF CERT:484726

Plugin Information

Published: 2012/01/04, Modified: 2024/10/07

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b  
Reported version : 0.9.6b  
Fixed version  : 0.9.6m
```

10.0.2.4 (tcp/443/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b  
Reported version : 0.9.6b  
Fixed version  : 0.9.6m
```


17756 (2) - OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability

Synopsis

The SSL layer on the remote server does not properly verify signatures.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7k or 0.9.8c.

These versions do not properly verify PKCS #1 v1.5 signatures and X509 certificates when the RSA exponent is 3.

See Also

<https://www.openssl.org/news/secadv/20060905.txt>

<https://www.us-cert.gov/ncas/alerts/ta06-333a>

Solution

Upgrade to OpenSSL 0.9.7k / 0.9.8c or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

2.4

EPSS Score

0.2763

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)

References

BID	19849
CVE	CVE-2006-4339
XREF	CERT:845620
XREF	CWE:310

Plugin Information

Published: 2012/01/04, Modified: 2024/10/23

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.7k
```

10.0.2.4 (tcp/443/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.7k
```

17759 (2) - OpenSSL < 0.9.8 Weak Default Configuration

Synopsis

The default configuration of OpenSSL on the remote server uses a weak hash algorithm.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8.

The default configuration uses MD5 instead of a stronger hash algorithm. An attacker could forge certificates.

If you never generate certificates on this machine, you may ignore this warning.

See Also

<https://bugs.launchpad.net/ubuntu/+source/openssl/+bug/19835>

<https://usn.ubuntu.com/179-1/>

Solution

Upgrade to OpenSSL 0.9.8 or later.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.003

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

CVE CVE-2005-2946

XREF CWE:310

Plugin Information

Published: 2012/01/04, Modified: 2024/10/23

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.8
```

10.0.2.4 (tcp/443/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.8
```

17765 (2) - OpenSSL < 0.9.8l Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8l. As such, it may be affected by multiple vulnerabilities :

- A remote attacker could crash the server by sending malformed ASN.1 data. This flaw only affects some architectures, Win64 and other unspecified platforms. (CVE-2009-0789)
- A remote attacker could saturate the server by sending a big number of 'future epoch' DTLS records. (CVE-2009-1377)
- A remote attacker could saturate the server by sending duplicate DTLS records, or DTLS records with too big sequence numbers. (CVE-2009-1378)
- A remote attacker could spoof certificates by computing MD2 hash collisions. (CVE-2009-2409)

See Also

<http://voodoo-circle.sourceforge.net/sa/sa-20090326-01.html>

<https://www.openssl.org/news/secadv/20090325.txt>

<http://voodoo-circle.sourceforge.net/sa/sa-20091012-01.html>

<http://cvs.openssl.org/chngview?cn=18187>

<http://cvs.openssl.org/chngview?cn=18188>

Solution

Upgrade to OpenSSL 0.9.8l or later.

Risk Factor

Medium

VPR Score

5.9

EPSS Score

0.105

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	34256
BID	35001
CVE	CVE-2009-0789
CVE	CVE-2009-1377
CVE	CVE-2009-1378
CVE	CVE-2009-2409
XREF	EDB-ID:8720
XREF	CWE:119
XREF	CWE:189
XREF	CWE:310
XREF	CWE:399

Plugin Information

Published: 2012/01/04, Modified: 2024/10/23

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.81
```

10.0.2.4 (tcp/443/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.81
```

88098 (2) - Apache Server ETag Header Information Disclosure

Synopsis

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

Description

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

See Also

<http://httpd.apache.org/docs/2.2/mod/core.html#FileETag>

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation 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

1.4

EPSS Score

0.001

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)

References

BID	6939
CVE	CVE-2003-1418
XREF	CWE:200

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/80/www)

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

```
Source           : ETag: "8805-b4a-3b96e9ae"  
Inode number     : 34821  
File size        : 2890 bytes  
File modification time : Sep.  6, 2001 at 03:12:46 GMT
```

10.0.2.4 (tcp/443/www)

Nessus was able to determine that the Apache Server listening on port 443 leaks the servers inode numbers in the ETag HTTP Header field :

```
Source           : ETag: "8805-b4a-3b96e9ae"  
Inode number     : 34821  
File size        : 2890 bytes  
File modification time : Sep.  6, 2001 at 03:12:46 GMT
```


193420 (2) - 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

0.0021

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

10.0.2.4 (tcp/80/www)

```
URL           : http://10.0.2.4/  
Installed version : 1.3.20  
Fixed version  : 2.4.54
```

10.0.2.4 (tcp/443/www)

```
URL           : https://10.0.2.4/  
Installed version : 1.3.20  
Fixed version  : 2.4.54
```

200201 (2) - OpenSSL 0.9.6 < 0.9.6j Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.6j. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.6j advisory.

- The SSL and TLS components for OpenSSL 0.9.6i and earlier, 0.9.7, and 0.9.7a allow remote attackers to perform an unauthorized RSA private key operation via a modified Bleichenbacher attack that uses a large number of SSL or TLS connections using PKCS #1 v1.5 padding that cause OpenSSL to leak information regarding the relationship between ciphertext and the associated plaintext, aka the Klima-Pokorny-Rosa attack. (CVE-2003-0131)
- OpenSSL does not use RSA blinding by default, which allows local and remote attackers to obtain the server's private key by determining factors using timing differences on (1) the number of extra reductions during Montgomery reduction, and (2) the use of different integer multiplication algorithms (Karatsuba and normal). (CVE-2003-0147)

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.cve.org/CVERecord?id=CVE-2003-0131>
<https://www.openssl.org/news/secadv/20030319.txt>
<https://www.cve.org/CVERecord?id=CVE-2003-0147>
<https://www.openssl.org/news/secadv/20030317.txt>

Solution

Upgrade to OpenSSL version 0.9.6j or later.

Risk Factor

High

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)

VPR Score

4.7

EPSS Score

0.2346

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-2003-0131

CVE CVE-2003-0147

Plugin Information

Published: 2024/06/07, Modified: 2024/10/07

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.6j
```

10.0.2.4 (tcp/443/www)

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.6j
```

200207 (2) - OpenSSL 0.9.6 < 0.9.6i Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.6i. It is, therefore, affected by a vulnerability as referenced in the 0.9.6i advisory.

- ssl3_get_record in s3_pkt.c for OpenSSL before 0.9.7a and 0.9.6 before 0.9.6i does not perform a MAC computation if an incorrect block cipher padding is used, which causes an information leak (timing discrepancy) that may make it easier to launch cryptographic attacks that rely on distinguishing between padding and MAC verification errors, possibly leading to extraction of the original plaintext, aka the Vaudenay timing attack. (CVE-2003-0078)

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.cve.org/CVERecord?id=CVE-2003-0078>

<https://www.openssl.org/news/secadv/20030219.txt>

Solution

Upgrade to OpenSSL version 0.9.6i 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

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

VPR Score

5.1

EPSS Score

0.0195

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

CVE CVE-2003-0078

Plugin Information

Published: 2024/06/07, Modified: 2024/10/07

Plugin Output

10.0.2.4 (tcp/80/www)

```
Banner          : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.6i
```

10.0.2.4 (tcp/443/www)

```
Banner          : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.6i
```

10802 (1) - OpenSSH < 3.0.1 Multiple Flaws

Synopsis

The remote host has an application that is affected by multiple vulnerabilities.

Description

According to its banner, the remote host appears to be running OpenSSH version 3.0.1 or older. Such versions are reportedly affected by multiple flaws :

- Provided KerberosV is enabled (disabled by default), it may be possible for an attacker to partially authenticate.
- It may be possible to crash the daemon due to a excessive memory clearing bug.

See Also

<https://seclists.org/bugtraq/2001/Nov/152>

Solution

Upgrade to OpenSSH 3.0.1 or later.

Risk Factor

Medium

VPR Score

4.7

EPSS Score

0.0063

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	3560
CVE	CVE-2001-1507

Plugin Information

Published: 2001/11/20, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 3.0.1
```


15901 (1) - 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

10.0.2.4 (tcp/443/www)

```
The SSL certificate has already expired :
```

```
Subject      : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit,
CN=localhost.localdomain, emailAddress=root@localhost.localdomain
Issuer       : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit,
CN=localhost.localdomain, emailAddress=root@localhost.localdomain
Not valid before : Sep 26 09:32:06 2009 GMT
Not valid after  : Sep 26 09:32:06 2010 GMT
```

26928 (1) - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

<http://www.nessus.org/u?6527892d>

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

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

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

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information

Published: 2007/10/08, Modified: 2021/02/03

Plugin Output

10.0.2.4 (tcp/443/www)

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

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
EXP-RC2-CBC-MD5 export	0x04, 0x00, 0x80	RSA(512)	RSA	RC2-CBC(40)	MD5
EXP-RC4-MD5 export	0x02, 0x00, 0x80	RSA(512)	RSA	RC4(40)	MD5
EXP-EDH-RSA-DES-CBC-SHA SHA1 export	0x00, 0x14	DH(512)	RSA	DES-CBC(40)	
EDH-RSA-DES-CBC-SHA SHA1	0x00, 0x15	DH	RSA	DES-CBC(56)	
EXP1024-DES-CBC-SHA SHA1 export	0x00, 0x62	RSA(1024)	RSA	DES-CBC(56)	
EXP1024-RC2-CBC-MD5 export	0x00, 0x61	RSA(1024)	RSA	RC2-CBC(56)	MD5
EXP1024-RC4-MD5 export	0x00, 0x60	RSA(1024)	RSA	RC4(56)	MD5
EXP1024-RC4-SHA SHA1 export	0x00, 0x64	RSA(1024)	RSA	RC4(56)	
EXP-DES-CBC-SHA SHA1 export	0x00, 0x08	RSA(512)	RSA	DES-CBC(40)	
EXP-RC2-CBC-MD5 export	0x00, 0x06	RSA(512)	RSA	RC2-CBC(40)	MD5
EXP-RC4-MD5 export	0x00, 0x03	RSA(512)	RSA	RC4(40)	MD5
DES-CBC-SHA SHA1	0x00, 0x09	RSA	RSA	DES-CBC(56)	

The fields above are :

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

31737 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 5.0
```

42880 (1) - SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Synopsis

The remote service allows insecure renegotiation of TLS / SSL connections.

Description

The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake.

An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.

See Also

<http://www.ietf.org/mail-archive/web/tls/current/msg03948.html>

<http://www.g-sec.lu/practicaltls.pdf>

<https://tools.ietf.org/html/rfc5746>

Solution

Contact the vendor for specific patch information.

Risk Factor

Medium

VPR Score

7.4

EPSS Score

0.0357

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

BID	36935
CVE	CVE-2009-3555
XREF	CERT:120541
XREF	CWE:310

Plugin Information

Published: 2009/11/24, Modified: 2020/06/12

Plugin Output

10.0.2.4 (tcp/443/www)

```
TLShv1 supports insecure renegotiation.
```

```
SSLv3 supports insecure renegotiation.
```

44065 (1) - 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

3.4

EPSS Score

0.6457

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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2  
Installed version   : 2.9p2  
Fixed version       : 5.2
```

44070 (1) - OpenSSH < 2.9.9p2 echo simulation Information Disclosure

Synopsis

The remote SSH service is affected by an information disclosure vulnerability.

Description

According to its banner, the remote host is running a version of OpenSSH earlier than 2.9.9p2. It therefore can potentially disclose the fact that the 'echo simulation' countermeasure is in use because the application sends an additional echo packet after the password and carriage return is entered.

Note that this issue only exists when the 'echo simulation' countermeasure is enabled.

Solution

Upgrade to OpenSSH 2.9.9p2 or later.

Risk Factor

Medium

VPR Score

5.3

EPSS Score

0.0053

CVSS v2.0 Base Score

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

References

CVE CVE-2001-1382

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 2.9.9p2 / 3.0
```

44073 (1) - OpenSSH With OpenPAM DoS

Synopsis

The SSH server running on the remote host has a denial of service vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is affected by a remote denial of service vulnerability. When used with OpenPAM, OpenSSH does not properly handle when a forked child process ends during PAM authentication. This could allow a remote attacker to cause a denial of service by connecting several times to the SSH server, waiting for the password prompt and then disconnecting.

See Also

https://bugzilla.mindrot.org/show_bug.cgi?id=839

<http://www.nessus.org/u?170f19e3>

Solution

Upgrade to OpenSSH 3.8.1p1 / 3.9 or later.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.0434

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 16892

CVE CVE-2006-0883

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 3.8.1p1 / 3.9
```

44074 (1) - Portable OpenSSH < 3.8p1 Multiple Vulnerabilities

Synopsis

Remote attackers may be able to cause information to leak from aborted sessions.

Description

According to its banner, a version of OpenSSH earlier than 3.8p1 is running on the remote host and is affected by the following issues:

- There is an issue in the handling of PAM modules in such versions of OpenSSH. As a result, OpenSSH may not correctly handle aborted conversations with PAM modules. Consequently, that memory may not be scrubbed of sensitive information such as credentials, which could lead to credentials leaking into swap space and core dumps. Other vulnerabilities in PAM modules could come to light because of unpredictable behavior.
- Denial of service attacks are possible when privilege separation is in use. This version of OpenSSH does not properly signal non-privileged processes after session termination when 'LoginGraceTime' is exceeded. This can allow connections to remain open thereby allowing the denial of service when resources are exhausted. (CVE-2004-2069)

See Also

<https://www.cl.cam.ac.uk/~mgk25/otpw.html#opensshbug>

https://bugzilla.mindrot.org/show_bug.cgi?id=632

<http://www.nessus.org/u?e86aec66>

<http://www.nessus.org/u?bbd79dfd>

<http://www.nessus.org/u?d2f25e5c>

Solution

Upgrade to OpenSSH 3.8p1 or later.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.0735

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	9040
BID	14963
CVE	CVE-2004-2069

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 3.8p1
```

44076 (1) - OpenSSH < 4.3 scp Command Line Filename Processing Command Injection

Synopsis

The version of SSH running on the remote host has a command injection vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is potentially affected by an arbitrary command execution vulnerability. The scp utility does not properly sanitize user-supplied input prior to using a system() function call. A local attacker could exploit this by creating filenames with shell metacharacters, which could cause arbitrary code to be executed if copied by a user running scp.

See Also

https://bugzilla.mindrot.org/show_bug.cgi?id=1094

<http://www.openssh.com/txt/release-4.3>

Solution

Upgrade to OpenSSH 4.3 or later.

Risk Factor

Medium

VPR Score

6.1

EPSS Score

0.0122

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 16369

CVE CVE-2006-0225

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 4.3
```

44079 (1) - 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

0.0394

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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 4.9
```

45411 (1) - 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

10.0.2.4 (tcp/443/www)

```
The identities known by Nessus are :
```

```
10.0.2.4  
10.0.2.4
```

```
The Common Name in the certificate is :
```

```
localhost.localdomain
```

51192 (1) - 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

10.0.2.4 (tcp/443/www)

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

```
| -Subject      : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/  
CN=localhost.localdomain/E=root@localhost.localdomain  
| -Not After    : Sep 26 09:32:06 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=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/  
CN=localhost.localdomain/E=root@localhost.localdomain  
| -Issuer       : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/  
CN=localhost.localdomain/E=root@localhost.localdomain
```

51892 (1) - OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue

Synopsis

The remote host allows resuming SSL sessions with a weaker cipher than the one originally negotiated.

Description

The version of OpenSSL on the remote host has been shown to allow resuming session with a weaker cipher than was used when the session was initiated. This means that an attacker that sees (i.e., by sniffing) the start of an SSL connection can manipulate the OpenSSL session cache to cause subsequent resumptions of that session to use a weaker cipher chosen by the attacker.

Note that other SSL implementations may also be affected by this vulnerability.

See Also

<https://www.openssl.org/news/secadv/20101202.txt>

Solution

Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.

Risk Factor

Medium

VPR Score

3.6

EPSS Score

0.1303

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	45164
CVE	CVE-2010-4180

Plugin Information

Published: 2011/02/07, Modified: 2022/04/11

Plugin Output

10.0.2.4 (tcp/443/www)

The server allowed the following session over TLSv1 to be resumed as follows :

```
Session ID      : d59275bbe13ded0a56678747924f4c81553061cbde76bac574e1dd22da4e873c
Initial Cipher  : TLS1_CK_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
Resumed Cipher  : TLS1_CK_RSA_EXPORT1024_WITH_RC4_56_SHA (0x0064)
```


57582 (1) - 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

10.0.2.4 (tcp/443/www)

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

```
| -Subject : C=-/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/  
CN=localhost.localdomain/E=root@localhost.localdomain
```

57608 (1) - 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

10.0.2.4 (tcp/139/smb)

65821 (1) - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

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

See Also

<https://www.rc4nomore.com/>

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

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

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0079

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/443/www)

List of RC4 cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-RC4-MD5 export	0x02, 0x00, 0x80	RSA (512)	RSA	RC4 (40)	MD5
EXP1024-RC4-MD5 export	0x00, 0x60	RSA (1024)	RSA	RC4 (56)	MD5
EXP1024-RC4-SHA SHA1 export	0x00, 0x64	RSA (1024)	RSA	RC4 (56)	
EXP-RC4-MD5 export	0x00, 0x03	RSA (512)	RSA	RC4 (40)	MD5

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RC4-MD5	0x01, 0x00, 0x80	RSA	RSA	RC4 (128)	MD5
RC4-MD5	0x00, 0x04	RSA	RSA	RC4 (128)	MD5
RC4-SHA SHA1	0x00, 0x05	RSA	RSA	RC4 (128)	

The fields above are :

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

67140 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 6.2
```

81606 (1) - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the-middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

See Also

<https://www.smacktls.com/#freak>

<https://www.openssl.org/news/secadv/20150108.txt>

<http://www.nessus.org/u?b78da2c4>

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Risk Factor

Medium

VPR Score

3.7

EPSS Score

0.9488

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 71936

CVE CVE-2015-0204
XREF CERT:243585

Plugin Information

Published: 2015/03/04, Modified: 2021/02/03

Plugin Output

10.0.2.4 (tcp/443/www)

EXPORT_RSA cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-DES-CBC-SHA SHA1 export	0x00, 0x08	RSA (512)	RSA	DES-CBC (40)	
EXP-RC2-CBC-MD5 export	0x00, 0x06	RSA (512)	RSA	RC2-CBC (40)	MD5
EXP-RC4-MD5 export	0x00, 0x03	RSA (512)	RSA	RC4 (40)	MD5

The fields above are :

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

85382 (1) - 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

0.3627

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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 7.0
```

89058 (1) - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

Synopsis

The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.

Description

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

See Also

<https://drownattack.com/>

<https://drownattack.com/drown-attack-paper.pdf>

Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

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)

VPR Score

3.6

EPSS Score

0.935

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)

References

BID 83733
CVE CVE-2016-0800
XREF CERT:583776

Plugin Information

Published: 2016/03/01, Modified: 2019/11/20

Plugin Output

10.0.2.4 (tcp/443/www)

The remote host is affected by SSL DROWN and supports the following vulnerable cipher suites :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-RC2-CBC-MD5 export	0x04, 0x00, 0x80	RSA (512)	RSA	RC2-CBC (40)	MD5
EXP-RC4-MD5 export	0x02, 0x00, 0x80	RSA (512)	RSA	RC4 (40)	MD5

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RC4-MD5	0x01, 0x00, 0x80	RSA	RSA	RC4 (128)	MD5

The fields above are :

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

90023 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 7.2p2 / 7.3
```

99359 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 7.5
```

103781 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 7.6
```

104743 (1) - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/443/www)

```
TLsv1 is enabled and the server supports at least one cipher.
```

159490 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 7.8
```

159491 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 8.0
```

187201 (1) - 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 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 distribution. (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

0.9486

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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 9.6p1 / 9.6
```

10114 (1) - 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

10.0.2.4 (icmp/0)

The difference between the local and remote clocks is -17986 seconds.

19592 (1) - OpenSSH < 4.2 Multiple Vulnerabilities

Synopsis

The remote SSH server has multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH installed on the remote host has the following vulnerabilities :

- X11 forwarding may be enabled unintentionally when multiple forwarding requests are made on the same session, or when an X11 listener is orphaned after a session goes away. (CVE-2005-2797)

- GSSAPI credentials may be delegated to users who log in using something other than GSSAPI authentication if 'GSSAPIDelegateCredentials' is enabled. (CVE-2005-2798)

- Attempting to log in as a nonexistent user causes the authentication process to hang, which could be exploited to enumerate valid user accounts.

Only OpenSSH on Mac OS X 10.4.x is affected.

(CVE-2006-0393)

- Repeatedly attempting to log in as a nonexistent user could result in a denial of service.

Only OpenSSH on Mac OS X 10.4.x is affected.

(CVE-2006-0393)

See Also

<http://www.openssh.com/txt/release-4.2>

<https://lists.apple.com/archives/security-announce/2006/Aug/msg00000.html>

<https://support.apple.com/?artnum=304063>

Solution

Upgrade to OpenSSH 4.2 or later. For OpenSSH on Mac OS X 10.4.x, apply Mac OS X Security Update 2006-004.

Risk Factor

Low

VPR Score

5.5

EPSS Score

0.0196

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	14727
BID	14729
BID	19289
CVE	CVE-2005-2797
CVE	CVE-2005-2798
CVE	CVE-2006-0393

Plugin Information

Published: 2005/09/07, Modified: 2024/03/27

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 4.2
```


44075 (1) - OpenSSH < 4.0 known_hosts Plaintext Host Information Disclosure

Synopsis

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

Description

According to its banner, the remote host is running a version of OpenSSH prior to 4.0. Versions of OpenSSH earlier than 4.0 are affected by an information disclosure vulnerability because the application stores hostnames, IP addresses, and keys in plaintext in the 'known_hosts' file. A local attacker, exploiting this flaw, could gain access to sensitive information that could be used in subsequent attacks.

See Also

<https://www.openssh.com/txt/release-4.0>

<http://nms.csail.mit.edu/projects/ssh/>

<http://www.eweek.com/c/a/Security/Researchers-Reveal-Holes-in-Grid/>

Solution

Upgrade to OpenSSH 4.0 or later.

Risk Factor

Low

VPR Score

5.5

EPSS Score

0.0085

CVSS v2.0 Base Score

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

References

CVE CVE-2005-2666

CVE CVE-2007-4654

CVE CVE-2004-2760

XREF CWE:16

XREF CWE:255

XREF

CWE:399

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 4.0
```

44080 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2  
Installed version   : 2.9p2  
Fixed version       : 5.1
```

53841 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
Version source      : SSH-1.99-OpenSSH_2.9p2
Installed version   : 2.9p2
Fixed version       : 5.8p2
```

78479 (1) - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

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

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

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

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

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

See Also

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00>

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.1

EPSS Score

0.9746

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	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/443/www)

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

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

83738 (1) - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

<https://weakdh.org/>

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

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

0.9698

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

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

References

BID 74733
CVE CVE-2015-4000
XREF CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/21, Modified: 2022/12/05

Plugin Output

10.0.2.4 (tcp/443/www)

EXPORT_DHE cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-EDH-RSA-DES-CBC-SHA	0x00, 0x14	DH(512)	RSA	DES-CBC(40)	
SHA1 export					

The fields above are :

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

83875 (1) - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

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

Description

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

See Also

<https://weakdh.org/>

Solution

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

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.5

EPSS Score

0.9698

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 74733
CVE CVE-2015-4000
XREF CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/28, Modified: 2024/09/11

Plugin Output

10.0.2.4 (tcp/443/www)

Vulnerable connection combinations :

SSL/TLS version : SSLv3
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

SSL/TLS version : TLSv1.0
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

11219 (6) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Port 22/tcp was found to be open
```

10.0.2.4 (tcp/80/www)

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

10.0.2.4 (tcp/111/rpc-portmapper)

```
Port 111/tcp was found to be open
```

10.0.2.4 (tcp/139/smb)

```
Port 139/tcp was found to be open
```

10.0.2.4 (tcp/443/www)

Port 443/tcp was found to be open

10.0.2.4 (tcp/32768/rpc-status)

Port 32768/tcp was found to be open

11111 (4) - 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

10.0.2.4 (tcp/111/rpc-portmapper)

The following RPC services are available on TCP port 111 :

- program: 100000 (portmapper), version: 2

10.0.2.4 (udp/111/rpc-portmapper)

The following RPC services are available on UDP port 111 :

- program: 100000 (portmapper), version: 2

10.0.2.4 (tcp/32768/rpc-status)

The following RPC services are available on TCP port 32768 :

- program: 100024 (status), version: 1

10.0.2.4 (udp/32768/rpc-status)

The following RPC services are available on UDP port 32768 :

- program: 100024 (status), version: 1

22964 (4) - 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

10.0.2.4 (tcp/22/ssh)

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

10.0.2.4 (tcp/80/www)

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

10.0.2.4 (tcp/443/www)

```
A TLSv1 server answered on this port.
```

10.0.2.4 (tcp/443/www)

```
A web server is running on this port through TLSv1.
```

10107 (2) - 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

10.0.2.4 (tcp/80/www)

```
The remote web server type is :  
Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
```

10.0.2.4 (tcp/443/www)

```
The remote web server type is :  
Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
```

11422 (2) - 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

10.0.2.4 (tcp/80/www)

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

10.0.2.4 (tcp/443/www)

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

24260 (2) - 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

10.0.2.4 (tcp/80/www)

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : GET, HEAD, OPTIONS, TRACE

Headers :

Date: Mon, 30 Dec 2024 20:44:21 GMT

Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

Last-Modified: Thu, 06 Sep 2001 03:12:46 GMT

ETag: "8805-b4a-3b96e9ae"

Accept-Ranges: bytes

Content-Length: 2890

Connection: close

Content-Type: text/html

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<HTML>

<HEAD>

<TITLE>Test Page for the Apache Web Server on Red Hat Linux</TITLE>

</HEAD>

```

<!-- Background white, links blue (unvisited), navy (visited), red (active) -->
<BODY BGCOLOR="#FFFFFF">

  <H1 ALIGN="CENTER">Test Page</H1>
  This page is used to test the proper operation of the Apache Web server after
  it has been installed.  If you can read this page, it means that the Apache
  Web server installed at this site is working properly.

  <HR WIDTH="50%">

  <H2 ALIGN="CENTER">If you are the administrator of this website:</H2>
  <P>
  You may now add content to this directory, and replace this page.  Note that
  until you do so, people visiting your website will see this page, and not your
  content.
  </P>

  <P>If you have upgraded from Red Hat Linux 6.2 and earlier, then you are
  seeing this page because the default <A
  href="manual/mod/core.html#documentroot"><STRONG>DocumentRoot</STRONG></A>
  set in <TT>/etc/httpd/conf/httpd.conf</TT> has changed.  Any subdirectories
  which existed under <TT>/home/httpd</TT> should now be moved to
  <TT>/var/www</TT>.  Alternatively, the contents of <TT>/var/www</TT> can be
  moved to <TT>/home/httpd</TT>, and the configuration file can be updated
  accordingly.
  </P>

  <HR WIDTH="50%">
  <H2 ALIGN="CENTER">If you are a member of the general public:</H2>

  <P>
  The fact that you are seeing this page indicates that the website you just
  visited is either experiencing problems, or is undergoing routine maintenance. [...]

```

10.0.2.4 (tcp/443/www)

Response Code : HTTP/1.0 200 OK

Protocol version : HTTP/1.0
 HTTP/2 TLS Support: No
 HTTP/2 Cleartext Support: No
 SSL : yes
 Keep-Alive : no
 Options allowed : GET, HEAD, OPTIONS, TRACE
 Headers :

Date: Mon, 30 Dec 2024 20:44:21 GMT
 Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
 Last-Modified: Thu, 06 Sep 2001 03:12:46 GMT
 ETag: "8805-b4a-3b96e9ae"
 Accept-Ranges: bytes
 Content-Length: 2890
 Connection: close
 Content-Type: text/html

Response Body :

```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<HTML>
  <HEAD>
    <TITLE>Test Page for the Apache Web Server on Red Hat Linux</TITLE>
  </HEAD>
  <!-- Background white, links blue (unvisited), navy (visited), red (active) -->
  <BODY BGCOLOR="#FFFFFF">

    <H1 ALIGN="CENTER">Test Page</H1>
    This page is used to test the proper operation of the Apache Web server after

```

it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

<HR WIDTH="50%">

<H2 ALIGN="CENTER">If you are the administrator of this website:</H2>

<P>

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

</P>

<P>If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default DocumentRoot set in <TT>/etc/httpd/conf/httpd.conf</TT> has changed. Any subdirectories which existed under <TT>/home/httpd</TT> should now be moved to <TT>/var/www</TT>. Alternatively, the contents of <TT>/var/www</TT> can be moved to <TT>/home/httpd</TT>, and the configuration file can be updated accordingly.

</P>

<HR WIDTH="50%">

<H2 ALIGN="CENTER">If you are a member of the general public:</H2>

<P>

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance [...]

43111 (2) - 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_\(OTG-CONFIG-006\)](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

10.0.2.4 (tcp/80/www)

Based on the response to an OPTIONS request :

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

10.0.2.4 (tcp/443/www)

Based on the response to an OPTIONS request :

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

48204 (2) - 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

10.0.2.4 (tcp/80/www)

```
URL      : http://10.0.2.4/
Version  : 1.3.20
Source   : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
backported : 0
modules  : (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
os       : Unix
```

10.0.2.4 (tcp/443/www)

```
URL      : https://10.0.2.4/
Version  : 1.3.20
```

```
Source      : Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
backported  : 0
modules     : (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
os          : Unix
```

57323 (2) - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

Nessus was able to extract the OpenSSL version from the web server's banner. Note that security patches in many cases are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

<https://www.openssl.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0682

Plugin Information

Published: 2011/12/16, Modified: 2024/11/14

Plugin Output

10.0.2.4 (tcp/80/www)

```
Source      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
```

10.0.2.4 (tcp/443/www)

```
Source      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
```

10150 (1) - 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

10.0.2.4 (udp/137/netbios-ns)

The following 7 NetBIOS names have been gathered :

KIOPTRIX	= Computer name
KIOPTRIX	= Messenger Service
KIOPTRIX	= File Server Service
__MSBROWSE__	= Master Browser
MYGROUP	= Workgroup / Domain name
MYGROUP	= Master Browser
MYGROUP	= Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.

10223 (1) - 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

10.0.2.4 (udp/111/rpc-portmapper)

10267 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
SSH version : SSH-1.99-OpenSSH_2.9p2
SSH supported authentication : publickey,password,keyboard-interactive
```

10287 (1) - 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

10.0.2.4 (udp/0)

For your information, here is the traceroute from 10.0.2.15 to 10.0.2.4 :

10.0.2.15

10.0.2.4

Hop Count: 1

10863 (1) - 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

10.0.2.4 (tcp/443/www)

```
Subject Name:

Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
Organization Unit: SomeOrganizationalUnit
Common Name: localhost.localdomain
Email Address: root@localhost.localdomain

Issuer Name:

Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
Organization Unit: SomeOrganizationalUnit
Common Name: localhost.localdomain
Email Address: root@localhost.localdomain

Serial Number: 00

Version: 3

Signature Algorithm: MD5 With RSA Encryption

Not Valid Before: Sep 26 09:32:06 2009 GMT
Not Valid After: Sep 26 09:32:06 2010 GMT

Public Key Info:
```



```
Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 CE 01 5E 22 B9 6D 69 52 A1 BE 01 E9 AF 40 2E 62 83 6D 2C
            6A A0 C7 0C DE 9B C6 1E C7 05 B0 9B 3E 7C 71 E7 F8 28 D4 D4
            35 F8 E0 B3 C3 34 EC 30 3A 5E 94 A9 BF 86 B5 92 6F EA 3B 95
            7A D0 F0 71 36 DB A1 C0 B6 04 CF BA C7 A8 32 57 F1 FA 69 8B
            82 B2 C0 B0 AC EB 95 29 6A 7B 97 DC 55 A5 A7 63 21 35 26 86
            1F AE 07 CD 6A CA AA 29 B7 FF D9 E1 31 F0 C3 B4 9E CC B2 50
            5E 2D 7E 1A B9 A9 DE 21 43
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 56 0A E6 A6 9A DF 92 67 7C BF 2D 04 D1 49 99 BD 67 48 70
            3A C8 61 1B D4 59 CC 12 17 07 3A 6C 6A 89 78 9A F4 09 84 81
            FA 30 D0 CC 0E 82 BB B9 ED C6 3A E5 5F 11 23 1C 50 41 6C 5E
            22 10 C2 43 9E E4 13 14 6B C8 09 02 1C AE A2 68 1F 79 6A 00
            EE F7 BB 84 DE 04 38 E1 BF 99 FE 87 E4 B7 EC 21 DD D6 5B E0
            46 0A 0E 6B 2F 5D 59 A2 CA 3B 25 13 86 02 85 D8 77 0F 58 C6
            48 8F 67 EB A2 8E 5E 8A 13

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: EC E7 51 4B 43 6B 6C D0 7C 80 4F 6A 52 37 30 F0 B1 7C C4 A0

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: EC E7 51 4B 43 6B 6C D0 7C 80 4F 6A 52 37 30 F0 B1 7C C4 A0
Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrg [...]
```

10881 (1) - 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

10.0.2.4 (tcp/22/ssh)

```
The remote SSH daemon supports the following versions of the
SSH protocol :
```

- 1.33
- 1.5
- 1.99
- 2.0

```
SSHv1 host key fingerprint : b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86
```

11011 (1) - 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

10.0.2.4 (tcp/139/smb)

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

11936 (1) - 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

10.0.2.4 (tcp/0)

```
Remote operating system : Linux Kernel 2.4  
Confidence level : 70  
Method : SinFP
```

```
The remote host is running Linux Kernel 2.4
```

19506 (1) - 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: 2024/10/04

Plugin Output

10.0.2.4 (tcp/0)

Information about this scan :

```
Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202412301102
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
```

```
Scan name : Kioptrix (1)
Scan policy used : Basic Network Scan
Scanner IP : 10.0.2.15
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 236.717 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/12/30 10:37 EST
Scan duration : 643 sec
Scan for malware : no
```

21643 (1) - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>

<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

10.0.2.4 (tcp/443/www)

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

SSL Version : TLSv1

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-EDH-RSA-DES-CBC-SHA SHA1 export	0x00, 0x14	DH(512)	RSA	DES-CBC(40)	
EDH-RSA-DES-CBC-SHA SHA1	0x00, 0x15	DH	RSA	DES-CBC(56)	
EXP1024-DES-CBC-SHA SHA1 export	0x00, 0x62	RSA(1024)	RSA	DES-CBC(56)	
EXP1024-RC2-CBC-MD5 export	0x00, 0x61	RSA(1024)	RSA	RC2-CBC(56)	MD5
EXP1024-RC4-MD5 export	0x00, 0x60	RSA(1024)	RSA	RC4(56)	MD5
EXP1024-RC4-SHA SHA1 export	0x00, 0x64	RSA(1024)	RSA	RC4(56)	
EXP-DES-CBC-SHA SHA1 export	0x00, 0x08	RSA(512)	RSA	DES-CBC(40)	

EXP-RC2-CBC-MD5 export	0x00, 0x06	RSA (512)	RSA	RC2-CBC (40)	MD5
EXP-RC4-MD5 export	0x00, 0x03	RSA (512)	RSA	RC4 (40)	MD5
DES-CBC-SHA SHA1	0x00, 0x09	RSA	RSA	DES-CBC (56)	

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

Name -----	Code -----	KEX ---	Auth ----	Encryption -----	MAC ---
EDH-RSA-DES-CBC3-SHA SHA1	0x00, 0x16	DH	RSA	3DES-CBC (168)	
DES-CBC3-SHA SHA1	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	

High Strength Ciphers (>= 112-bit key)

Name	Code	[...]
------	------	-------

25220 (1) - 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

10.0.2.4 (tcp/0)

35716 (1) - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/0)

The following card manufacturers were identified :

08:00:27:2E:20:D4 : PCS Systemtechnik GmbH

45410 (1) - 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

10.0.2.4 (tcp/443/www)

The host name known by Nessus is :

kioptrix

The Common Name in the certificate is :

localhost.localdomain

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

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

Description

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

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

See Also

<http://cpe.mitre.org/>

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/11/22

Plugin Output

10.0.2.4 (tcp/0)

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:1.3.20 -> Apache Software Foundation Apache HTTP Server

cpe:/a:modssl:mod_ssl:2.8.4 -> mod_ssl

cpe:/a:openbsd:openssh:2.9p2 -> OpenBSD OpenSSH

cpe:/a:openssl:openssl:0.9.6b -> OpenSSL Project OpenSSL

51891 (1) - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/443/www)

```
This port supports resuming SSLv3 / TLSv1 sessions.
```

53335 (1) - 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

10.0.2.4 (tcp/111/rpc-portmapper)

53360 (1) - SSL Server Accepts Weak Diffie-Hellman Keys

Synopsis

The remote SSL/TLS server accepts a weak Diffie-Hellman public value.

Description

The remote SSL/TLS server accepts a weak Diffie-Hellman (DH) public key value.

This flaw may aid an attacker in conducting a man-in-the-middle (MiTM) attack against the remote server since it could enable a forced calculation of a fully predictable Diffie-Hellman secret.

By itself, this flaw is not sufficient to set up a MiTM attack (hence a risk factor of 'None'), as it would require some SSL implementation flaws to affect one of the clients connecting to the remote host.

See Also

<https://www.cl.cam.ac.uk/~rja14/Papers/psandqs.pdf>

<https://tls.mbed.org/tech-updates/security-advisories/polarssl-security-advisory-2011-01>

Solution

OpenSSL is affected when compiled in FIPS mode. To resolve this issue, either upgrade to OpenSSL 1.0.0, disable FIPS mode or configure the ciphersuite used by the server to not include any Diffie-Hellman key exchanges.

PolarSSL is affected. To resolve this issue, upgrade to version 0.99-pre3 / 0.14.2 or higher.

If using any other SSL implementation, configure the ciphersuite used by the server to not include any Diffie-Hellman key exchanges or contact your vendor for a patch.

Risk Factor

None

Plugin Information

Published: 2011/04/11, Modified: 2020/06/12

Plugin Output

10.0.2.4 (tcp/443/www)

```
It was possible to complete a full SSL handshake by sending a DH key
with a value of 1.
```

54615 (1) - 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

10.0.2.4 (tcp/0)

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


56984 (1) - 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

10.0.2.4 (tcp/443/www)

```
This port supports SSLv2/SSLv3/TLSv1.0.
```

57041 (1) - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/443/www)

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

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
EXP-EDH-RSA-DES-CBC-SHA SHA1 export	0x00, 0x14	DH(512)	RSA	DES-CBC(40)	
EDH-RSA-DES-CBC-SHA SHA1	0x00, 0x15	DH	RSA	DES-CBC(56)	

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---

EDH-RSA-DES-CBC3-SHA	0x00, 0x16	DH	RSA	3DES-CBC(168)
SHA1				

The fields above are :

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

58768 (1) - SSL Resume With Different Cipher Issue

Synopsis

The remote host allows resuming SSL sessions with a different cipher than the one originally negotiated.

Description

The SSL implementation on the remote host has been shown to allow a cipher other than the one originally negotiated when resuming a session. An attacker that sees (e.g. by sniffing) the start of an SSL connection may be able to manipulate session cache to cause subsequent resumptions of that session to use a cipher chosen by the attacker.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/04/17, Modified: 2012/04/17

Plugin Output

10.0.2.4 (tcp/443/www)

The server allowed the following session over TLSv1 to be resumed as follows :

```
Session ID      : d59275bbe13ded0a56678747924f4c81553061cbde76bac574e1dd22da4e873c
Initial Cipher  : TLS1_CK_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
Resumed Cipher  : TLS1_CK_RSA_EXPORT1024_WITH_RC4_56_SHA (0x0064)
```

66334 (1) - Patch Report

Synopsis

The remote host is missing several patches.

Description

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

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/12/10

Plugin Output

10.0.2.4 (tcp/0)

. You need to take the following 3 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 27 different vulnerabilities (CVEs).

[OpenSSH < 9.6 Multiple Vulnerabilities (187201)]

+ Action to take : Upgrade to OpenSSH version 9.6 or later.

+Impact : Taking this action will resolve 55 different vulnerabilities (CVEs).

[OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue (51892)]

+ Action to take : Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.

+Impact : Taking this action will resolve 19 different vulnerabilities (CVEs).

70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>

<http://www.nessus.org/u?cc4a822a>

<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/443/www)

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

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
EXP-RC2-CBC-MD5 export	0x04, 0x00, 0x80	RSA(512)	RSA	RC2-CBC(40)	MD5
EXP-EDH-RSA-DES-CBC-SHA SHA1 export	0x00, 0x14	DH(512)	RSA	DES-CBC(40)	
EDH-RSA-DES-CBC-SHA SHA1	0x00, 0x15	DH	RSA	DES-CBC(56)	
EXP1024-DES-CBC-SHA SHA1 export	0x00, 0x62	RSA(1024)	RSA	DES-CBC(56)	
EXP1024-RC2-CBC-MD5 export	0x00, 0x61	RSA(1024)	RSA	RC2-CBC(56)	MD5

EXP-DES-CBC-SHA SHA1	0x00, 0x08	RSA (512)	RSA	DES-CBC (40)	
EXP-RC2-CBC-MD5 export	0x00, 0x06	RSA (512)	RSA	RC2-CBC (40)	MD5
DES-CBC-SHA SHA1	0x00, 0x09	RSA	RSA	DES-CBC (56)	

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
DES-CBC3-MD5	0x07, 0x00, 0xC0	RSA	RSA	3DES-CBC (168)	MD5
EDH-RSA-DES-CBC3-SHA SHA1	0x00, 0x16	DH	RSA	3DES-CBC (168)	
DES-CBC3-SHA SHA1	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	

The fields above are :

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


84502 (1) - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

<https://tools.ietf.org/html/rfc6797>

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

10.0.2.4 (tcp/443/www)

```
HTTP/1.0 200 OK
Date: Mon, 30 Dec 2024 20:43:20 GMT
Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Last-Modified: Thu, 06 Sep 2001 03:12:46 GMT
ETag: "8805-b4a-3b96e9ae"
Accept-Ranges: bytes
Content-Length: 2890
Connection: close
Content-Type: text/html
```

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

86420 (1) - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/0)

```
The following is a consolidated list of detected MAC addresses:  
- 08:00:27:2E:20:D4
```

94761 (1) - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10))

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

10.0.2.4 (tcp/443/www)

The following root Certification Authority certificate was found :

```
| -Subject          : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/  
CN=localhost.localdomain/E=root@localhost.localdomain  
| -Issuer          : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/  
CN=localhost.localdomain/E=root@localhost.localdomain  
| -Valid From      : Sep 26 09:32:06 2009 GMT  
| -Valid To       : Sep 26 09:32:06 2010 GMT  
| -Signature Algorithm : MD5 With RSA Encryption
```

106716 (1) - 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

10.0.2.4 (tcp/139/smb)

```
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
```

110723 (1) - 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

10.0.2.4 (tcp/0)

SSH was detected on port 22 but no credentials were provided.

SSH local checks were not enabled.

117886 (1) - 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

10.0.2.4 (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.
```

135860 (1) - 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 vulnerabilities that exist on the remote host.

See Also

<https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2024/11/22

Plugin Output

10.0.2.4 (tcp/139/smb)

```
Can't connect to the 'root\CIMV2' WMI namespace.
```


149334 (1) - 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

10.0.2.4 (tcp/22/ssh)

156899 (1) - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

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

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

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

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

Plugin Output

10.0.2.4 (tcp/443/www)

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

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
EXP-RC2-CBC-MD5 export	0x04, 0x00, 0x80	RSA(512)	RSA	RC2-CBC(40)	MD5
EXP-RC4-MD5 export	0x02, 0x00, 0x80	RSA(512)	RSA	RC4(40)	MD5
EXP-EDH-RSA-DES-CBC-SHA SHA1 export	0x00, 0x14	DH(512)	RSA	DES-CBC(40)	
EDH-RSA-DES-CBC-SHA SHA1	0x00, 0x15	DH	RSA	DES-CBC(56)	
EXP1024-DES-CBC-SHA SHA1 export	0x00, 0x62	RSA(1024)	RSA	DES-CBC(56)	
EXP1024-RC2-CBC-MD5 export	0x00, 0x61	RSA(1024)	RSA	RC2-CBC(56)	MD5
EXP1024-RC4-MD5 export	0x00, 0x60	RSA(1024)	RSA	RC4(56)	MD5
EXP1024-RC4-SHA SHA1 export	0x00, 0x64	RSA(1024)	RSA	RC4(56)	
EXP-DES-CBC-SHA SHA1 export	0x00, 0x08	RSA(512)	RSA	DES-CBC(40)	
EXP-RC2-CBC-MD5 export	0x00, 0x06	RSA(512)	RSA	RC2-CBC(40)	MD5
EXP-RC4-MD5 export	0x00, 0x03	RSA(512)	RSA	RC4(40)	MD5
DES-CBC-SHA SHA1	0x00, 0x09	RSA	RSA	DES-CBC(56)	

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
DES-CBC3-MD5	0x07, 0x00, 0xC0	RSA	RSA	3DES-CBC(168) [...]	

181418 (1) - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

<https://www.openssh.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2024/12/18

Plugin Output

10.0.2.4 (tcp/22/ssh)

```
Service : ssh
Version : 2.9p2
Banner  : SSH-1.99-OpenSSH_2.9p2
```