Vulnerability Assessment after Remediation

Wed, 30 Aug 2023 09:16:54 EDT

Vulnerabilities by Host 192.168.50.100

8	10	37	10	96
CRITICAL	HIGH	MEDIUM	LOW	INFO

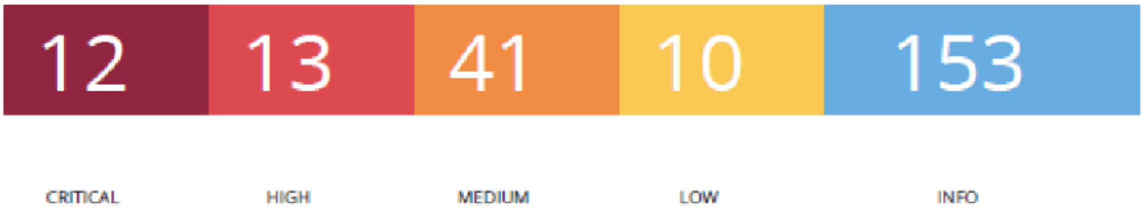
Scan Information

Start time:	Wed Aug 30 07:56:11 2023
End time:	Wed Aug 30 09:16:54 2023

Host Information

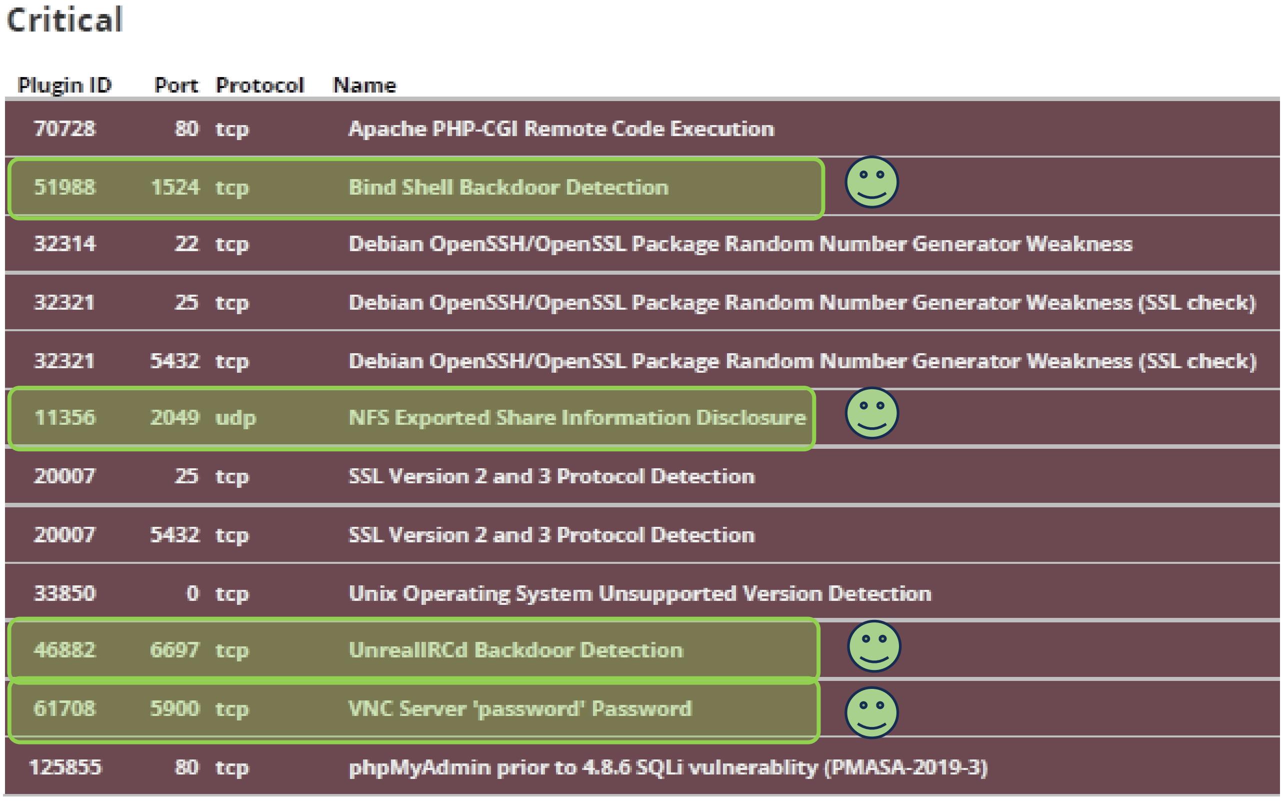
Netbios Name:	METASPLOITABLE
IP:	192.168.50.100
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

A seguito delle azioni di rimedio intraprese a valle della vulnerability scan iniziale, che ha riportato i seguenti risultati:



12	13	41	10	153
CRITICAL	HIGH	MEDIUM	LOW	INFO

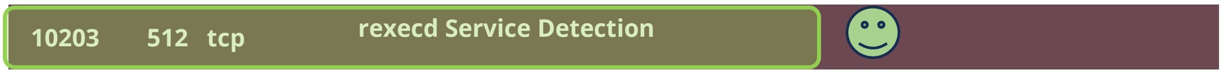
Sono state intraprese delle remediation actions che hanno risolto le seguenti 4 vulnerabilità critiche rilevate nella scansione precedente:



Critical

Plugin ID	Port	Protocol	Name	
70728	80	tcp	Apache PHP-CGI Remote Code Execution	
51988	1524	tcp	Bind Shell Backdoor Detection	☺
32314	22	tcp	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	
32321	25	tcp	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	
32321	5432	tcp	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	
11356	2049	udp	NFS Exported Share Information Disclosure	☺
20007	25	tcp	SSL Version 2 and 3 Protocol Detection	
20007	5432	tcp	SSL Version 2 and 3 Protocol Detection	
33850	0	tcp	Unix Operating System Unsupported Version Detection	
46882	6697	tcp	UnrealIRCd Backdoor Detection	☺
61708	5900	tcp	VNC Server 'password' Password	☺
125855	80	tcp	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)	

oltre alla seguente vulnerabilità critica non rilevata nella scansione iniziale, ma ben nota e verificata, che è stata risolta anche per la porta TCP 513:



10203	512	tcp	rexecd Service Detection	☺

Si riporta di seguito un ripeilogo delle vulnerabilità critiche residue, rilevate dalla scasione successiva alle remerìdiation actions.

Critical

Plugin ID	Name
70728	Apache PHP-CGI Remote Code Execution
134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
20007	SSL Version 2 and 3 Protocol Detection
125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
171340	Apache Tomcat SEoL (<= 5.5.x)
33850	Unix Operating System Unsupported Version Detection
32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
32321	Unix Operating System Unsupported Version Detection

70728 Apache PHPCGI Remote Code Execution

Synopsis

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

Description

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

Solution

Upgrade to PHP 5.3.13 / 5.4.3 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	53388
CVE	CVE20121823
CVE	CVE20122311
CVE	CVE20122335
CVE	CVE20122336
XREF	CERT:520827
XREF	EDBID:29290
XREF	EDBID:29316
XREF	CISAKNOWNEXPLOITED:2022/04/15

Exploitable With

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

Plugin Information

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

Plugin Output

tcp/80/www

134862 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 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 v2.0 Base Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)4

CVSS v2.0 Temporal Score

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

Plugin Information

Published: 2020/03/24, Modified: 2023/07/17

Plugin Output

tcp/8009/ajp13

20007 SSL Version 2 and 3 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: An insecure padding scheme with CBC ciphers. Insecure session renegotiation and resumption schemes.An attacker can exploit these flaws to conduct maninthemiddle 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/paperssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/sslpoodle.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:C/I:C/A:C)

Plugin Information

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

Plugin Output

tcp/5432/postgresql

125855 phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA20193)

Synopsis

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

Description

According to its selfreported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the backend database, resulting in the disclosure or manipulation of arbitrary data.Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's selfreported version number.

See Also

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

Solution

Upgrade to phpMyAdmin version 4.8.6 or later.Alternatively, apply the patches referenced in the vendor advisories.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	108617
CVE	CVE201911768

Plugin Information

Published: 2019/06/13, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL : http://192.168.50.100/phpMyAdminInstalled version : 3.1.1Fixed version : 4.8.6
```

171340 Apache Tomcat SEoL (<= 5.5.x)

Synopsis

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

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

Risk Factor

Critical

CVSS v2.0 Base Score

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

Plugin Information

Published: 2023/02/10, Modified: 2023/06/13

Plugin Output

tcp/8180/www

33850 Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its selfreported version number, the Unix operating system running on the remote host is no longer supported.Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	IAVA:0001A0502
XREF	IAVA:0001A0648

Plugin Information

Published: 2008/08/08, Modified: 2023/07/07

Plugin Output

tcp/0

32314 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Solution

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

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE20080166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2018/11/15

Plugin Output

tcp/22/ssh

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

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Solution

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

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE20080166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

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

Plugin Output

tcp/25/smtp

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

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Solution

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

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE20080166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

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

Plugin Output

tcp/5432/postgresql