Obiettivo: Esercizio di Vulnerability Scanning

Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, configurare scansioni mirate e familiarizzare con alcune delle vulnerabilità più note. *solo su porti comuni*

Obiettivo: Analisi del Report

Lo studente, al termine della scansione, scaricherà e analizzerà il report generato da Nessus. In questa fase, l'attenzione sarà posta sulla comprensione e l'approfondimento delle vulnerabilità identificate.

Questo esercizio rafforzerà le competenze tecniche nell'utilizzo di Nessus, nell'interpretazione dei report e nell'approfondimento delle vulnerabilità identificate.

Dopo aver selezionato il nostro target (Metasploitable 2 192.168.1.15) nella scheda discovery ho impostato l'assesments per scannerizzare solo le porte comuni di default come richiesto dall'esercizio. una volta date le regole da seguire per la scansione delle porte (in questo caso un port scan delle porte comuni e non di tutte) Ho esportato le vulnerabilità in formato pdf leggibile per un report accurato. In ordine: Common port scan, all web vulnerabilities Quick/ All port scan All web vulnerabilities Complex per vedere le differenze.

vulnerabilità piu critiche individuate e analizzate (Completamento dell'esercizio):

- Apache PHP-CGI Remote Code Execution: Consente l'esecuzione remota di comandi sul server tramite PHP-CGI.
- Bind Shell Backdoor Detection: Rileva una shell di backdoor che offre accesso remoto al sistema.
- SSL Version 2 and 3 Protocol Detection: Identifica l'uso di protocolli SSL vulnerabili ad attacchi man-in-the-middle.
- phpMyAdmin SQL Injection: Consente SQL injection su versioni precedenti alla 4.8.6, permettendo accesso al database.
- Debian OpenSSH/OpenSSL Weakness: Rileva chiavi SSH deboli a causa di un bug OpenSSL, esponendo le sessioni a decrittazione.
- UnrealIRCd Backdoor Detection: Individua una backdoor in UnrealIRCd che permette esecuzione arbitraria di codice.
- VNC Server Weak Password: Il server VNC è protetto con la password debole "password", facilmente accessibile.
- Debian OpenSSL Weak Key (SSL check): Rileva certificati SSL deboli generati con poca entropia, facilitando la decrittazione.facilmente accessibile
- Samba Badlock Vulnerability Questa vulnerabilità, permette l'attacco"man-in-the-middle" di eseguire comandi arbitrari sulla rete Samba.

Queste vulnerabilità rappresentano rischi di sicurezza molto, molto gravi e possono facilitare l'accesso non autorizzato e la compromissione del sistema.

Esercizio extra: Vulnerability scan all ports and complex mode.

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Consente la lettura di file non autorizzata e l'esecuzione di codice remoto se sono possibili upload di file.

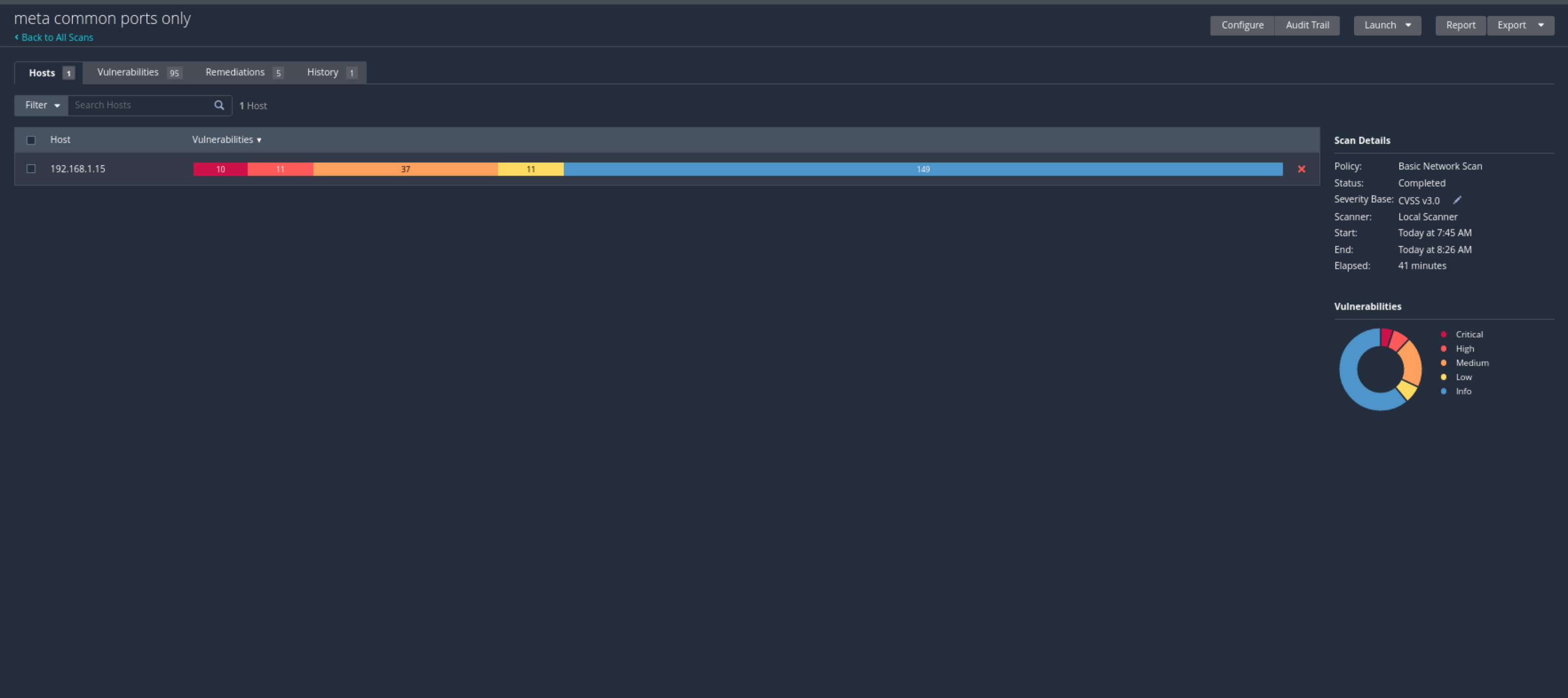
Apache Tomcat SEoL (<= 5.5.x)

Versione non più supportata e senza aggiornamenti di sicurezza, suscettibile a potenziali exploit.

NFS Shares World Readable

Il server *NFS* esporta condivisioni senza restrizioni di accesso, rendendo i file leggibili a tutti.

Oltre le altre vulnerabilità critiche elencate sopra su common ports, queste sono in più. Trovate con il deepscan complex e il range delle porte totali (65535)

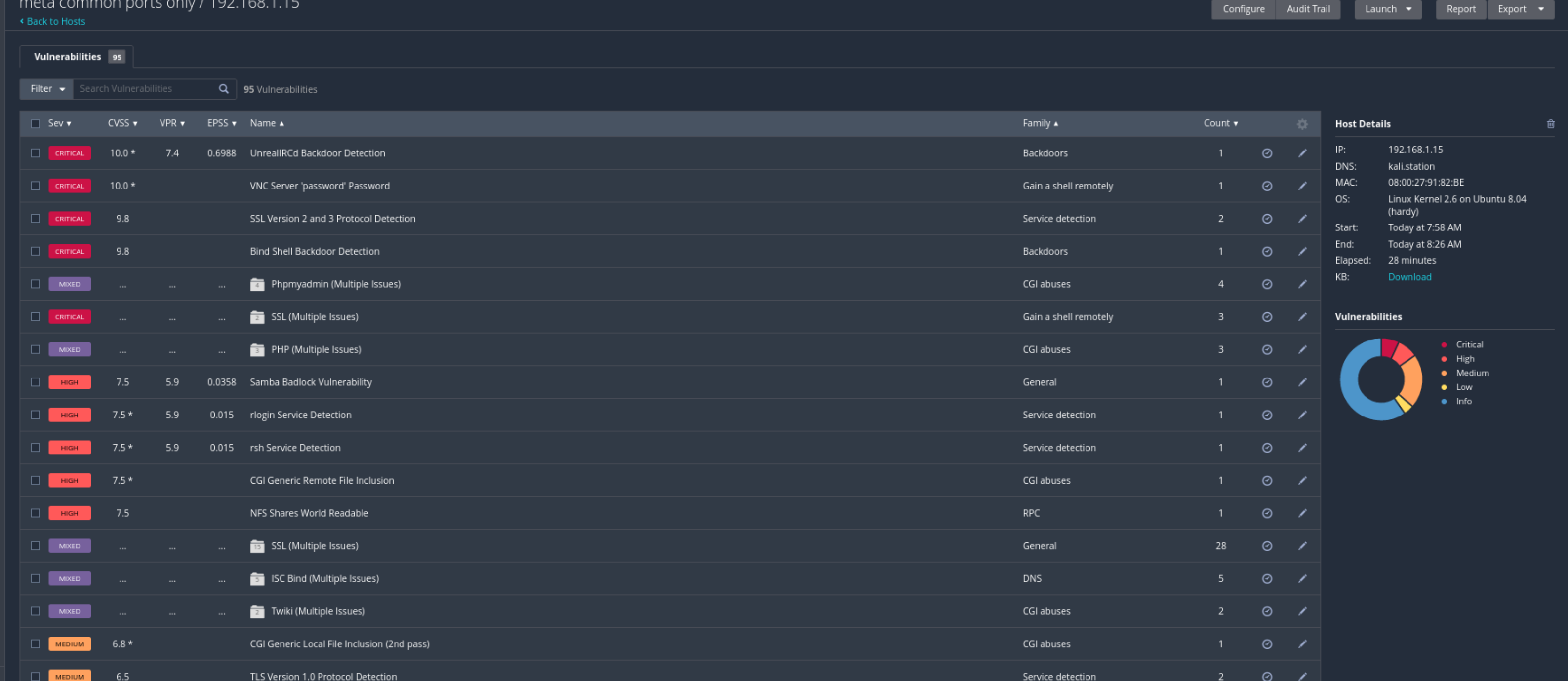


□ Host	Vulnerabilities ▾
□ 192.168.1.15	10 · 11 · 37 · 11 · 149

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:45 AM
End:	Today at 8:26 AM
Elapsed:	41 minutes

Vulnerabilities



meta common ports only / 192.168.1.15

‹ Back to Hosts

Vulnerabilities 95

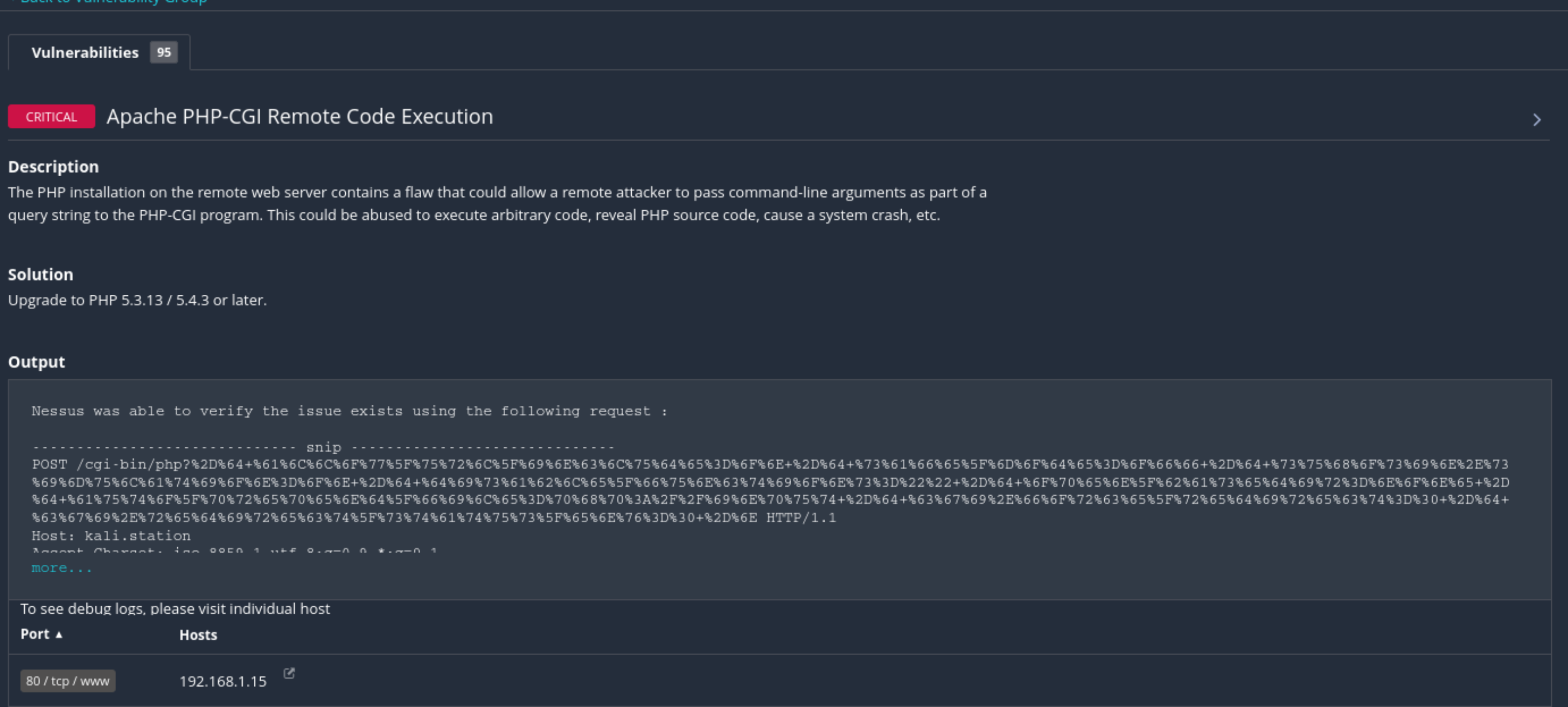
95 Vulnerabilities

□	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
□	CRITICAL	10.0 *	7.4	0.6988	UnrealIRCd Backdoor Detection	Backdoors	1
□	CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
□	CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
□	CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
□	MIXED	...	...	...	Phpmyadmin (Multiple Issues)	CGI abuses	4
□	CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
□	MIXED	...	...	...	PHP (Multiple Issues)	CGI abuses	3
□	HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1
□	HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1
□	HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1
□	HIGH	7.5 *			CGI Generic Remote File Inclusion	CGI abuses	1
□	HIGH	7.5			NFS Shares World Readable	RPC	1
□	MIXED	...	...	...	SSL (Multiple Issues)	General	28
□	MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
□	MIXED	...	...	...	Twiki (Multiple Issues)	CGI abuses	2
□	MEDIUM	6.8 *			CGI Generic Local File Inclusion (2nd pass)	CGI abuses	1
□	MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2

Host Details

IP:	192.168.1.15
DNS:	kali.station
MAC:	08:00:27:91:82:BE
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 7:58 AM
End:	Today at 8:26 AM
Elapsed:	28 minutes
KB:	Download

Vulnerabilities



CRITICAL Apache PHP-CGI Remote Code Execution

Description

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

Solution

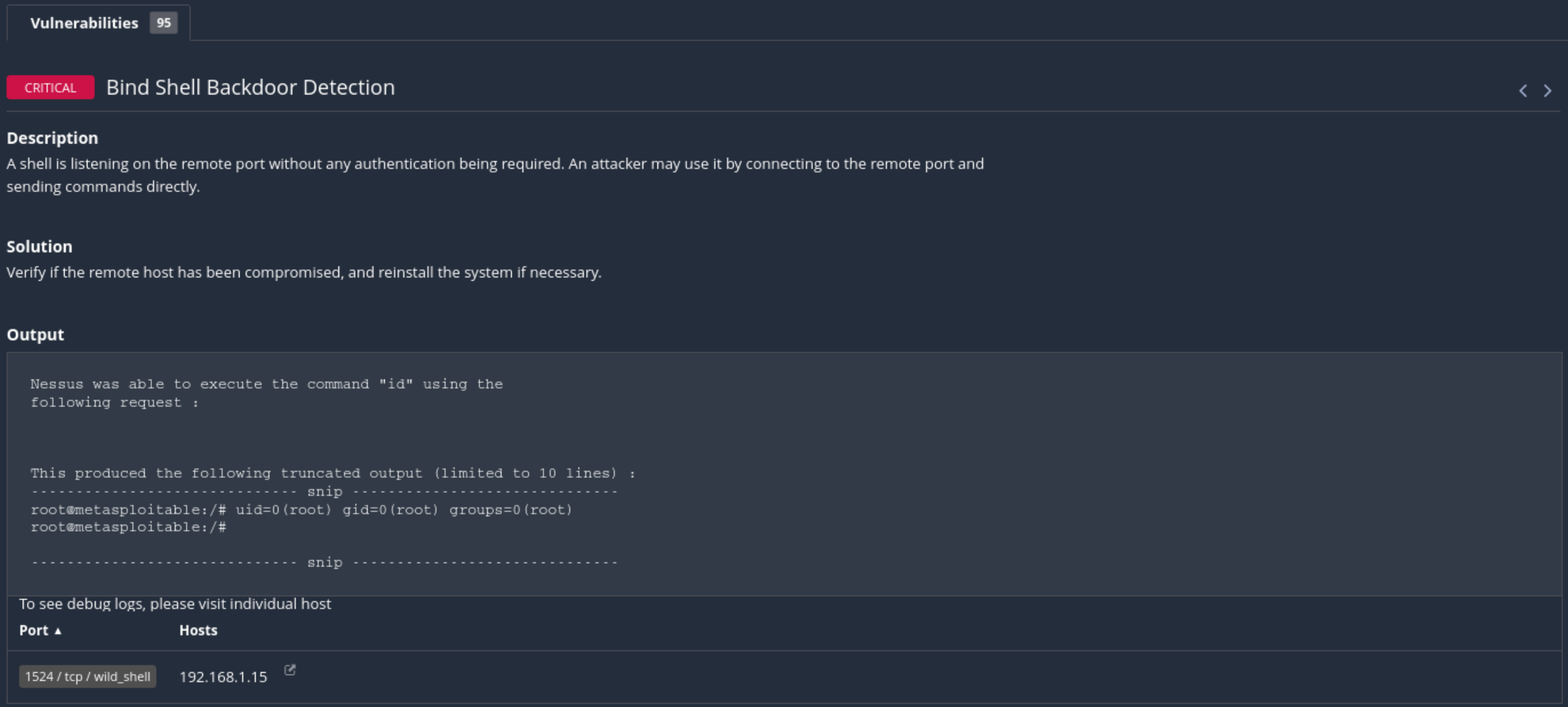
Upgrade to PHP 5.3.13 / 5.4.3 or later.

Output

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

------------------------------ snip ------------------------------
POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73
%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D
%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+
%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E HTTP/1.1
Host: kali.station
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
```

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	192.168.1.15



Vulnerabilities 95

CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

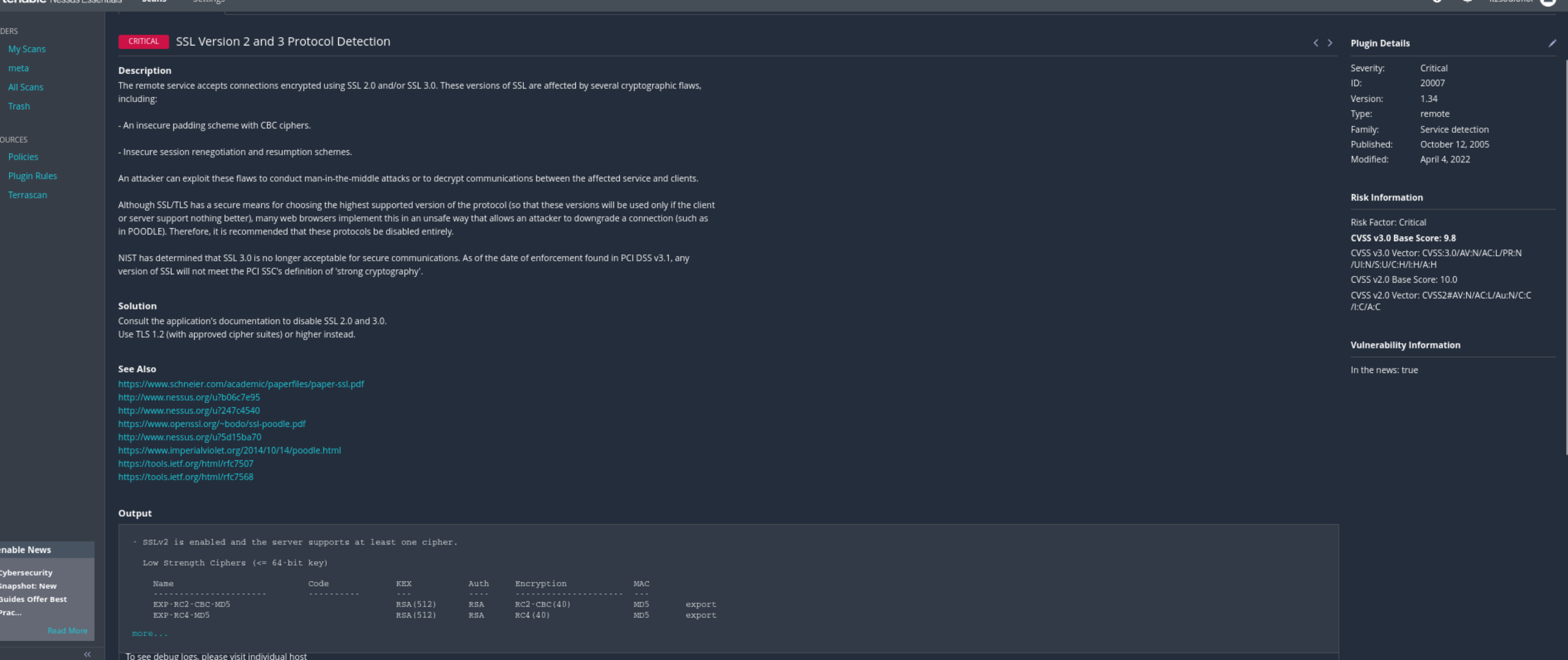
Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :



This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

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

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.1.15



CRITICAL SSL Version 2 and 3 Protocol Detection

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'.

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.

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

Output

```
  - 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                                RSA(512)      RSA      RC2-CBC(40)            MD5      export
      EXP-RC4-MD5                                    RSA(512)      RSA      RC4(40)                MD5      export

  more...
```

To see debug logs, please visit individual host

Plugin Details

Severity:	Critical
ID:	20007
Version:	1.34
Type:	remote
Family:	Service detection
Published:	October 12, 2005
Modified:	April 4, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score: 9.8

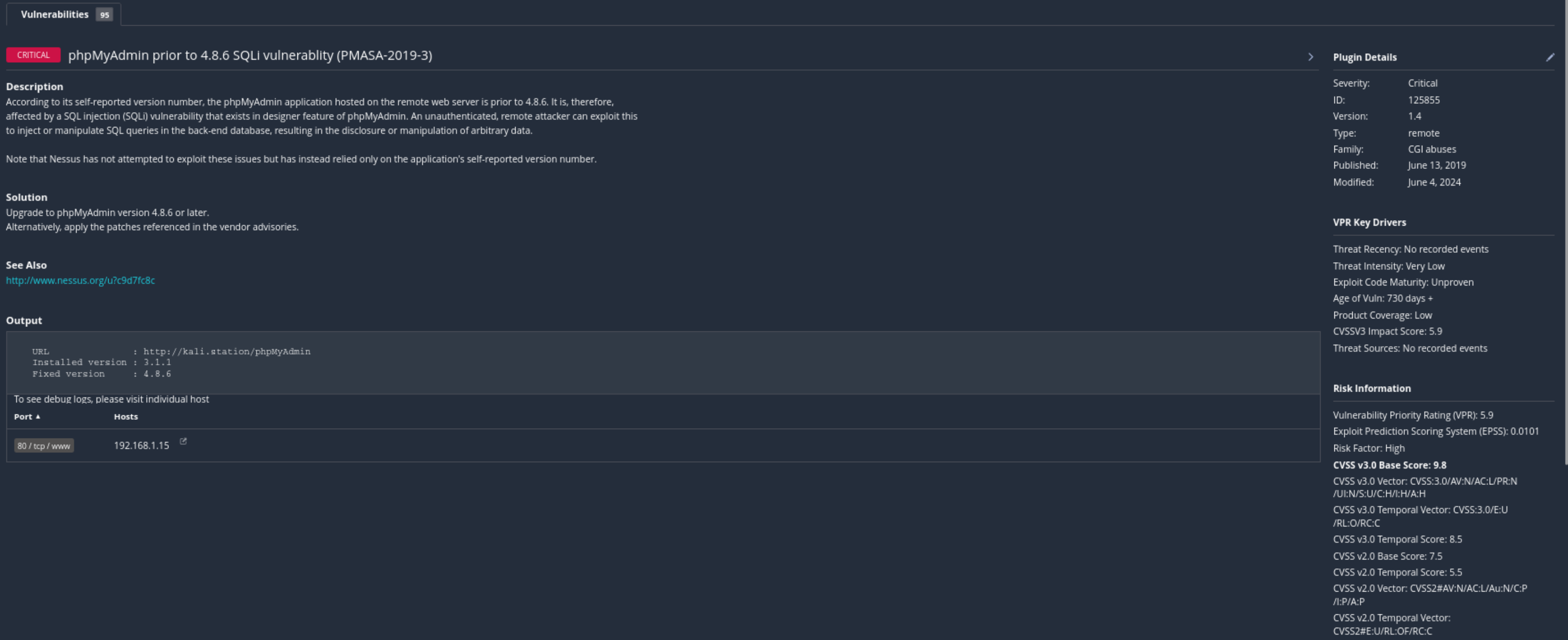
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

In the news: true



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

Description

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

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

Solution

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

See Also

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

Output

```
  URL               : http://kali.station/phpMyAdmin
  Installed version : 3.1.1
  Fixed version     : 4.8.6
```

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	192.168.1.15

Plugin Details

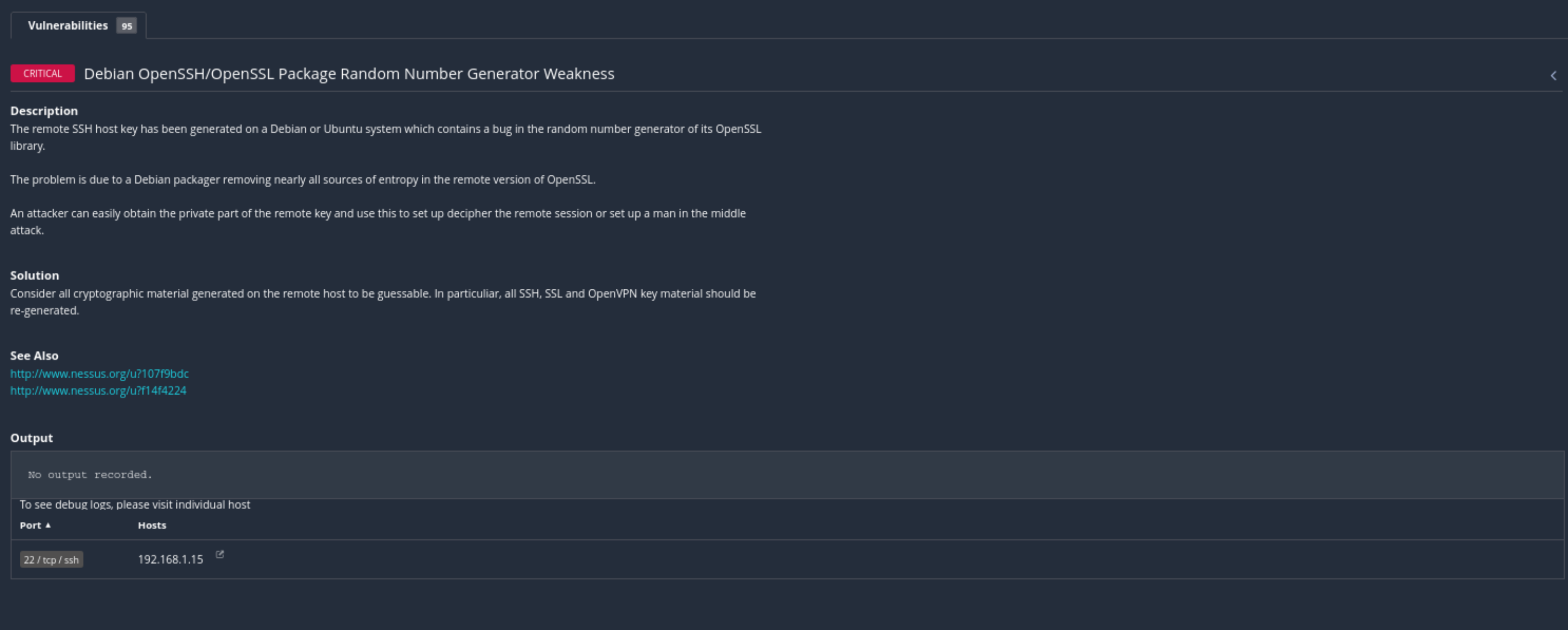
Severity:	Critical
ID:	125855
Version:	1.4
Type:	remote
Family:	CGI abuses
Published:	June 13, 2019
Modified:	June 4, 2024

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Exploit Prediction Scoring System (EPSS): 0.0101
Risk Factor: High
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 8.5
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Temporal Score: 5.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C



CRITICAL

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

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.

Solution

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

See Also

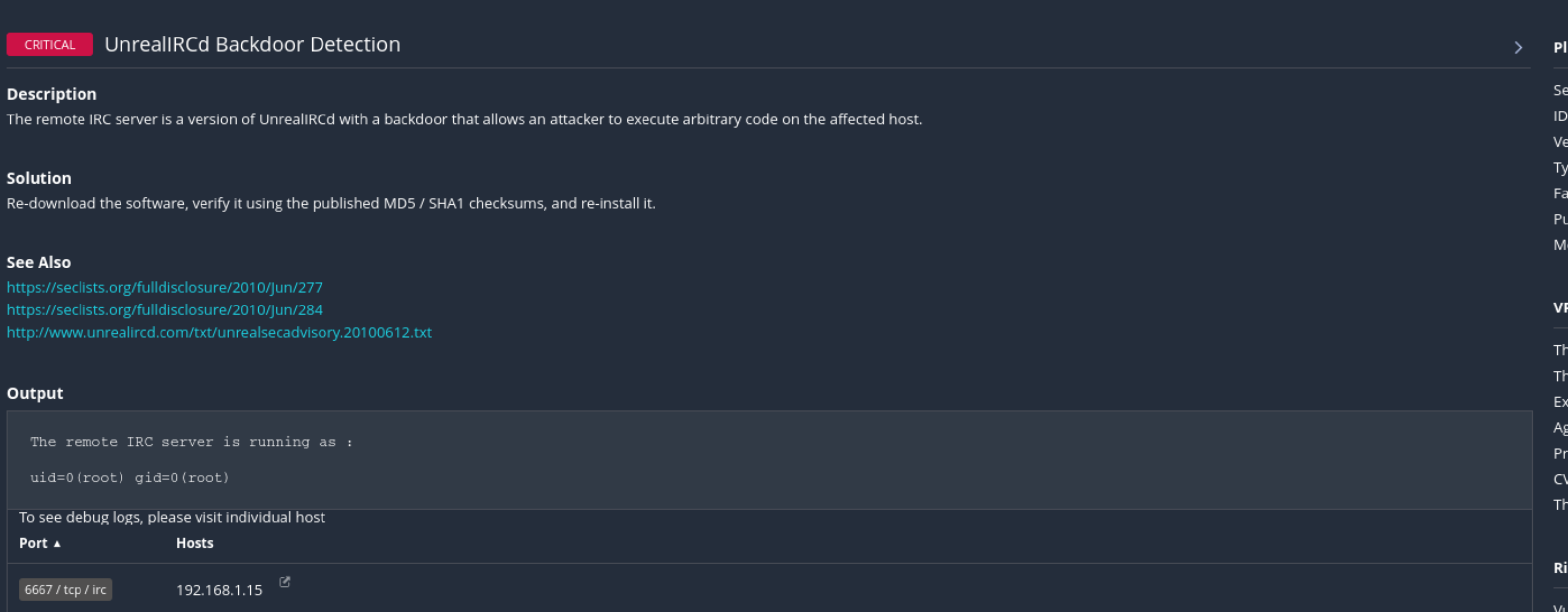
http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▲	Hosts
22 / tcp / ssh	192.168.1.15



CRITICAL

UnrealIRCd Backdoor Detection

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

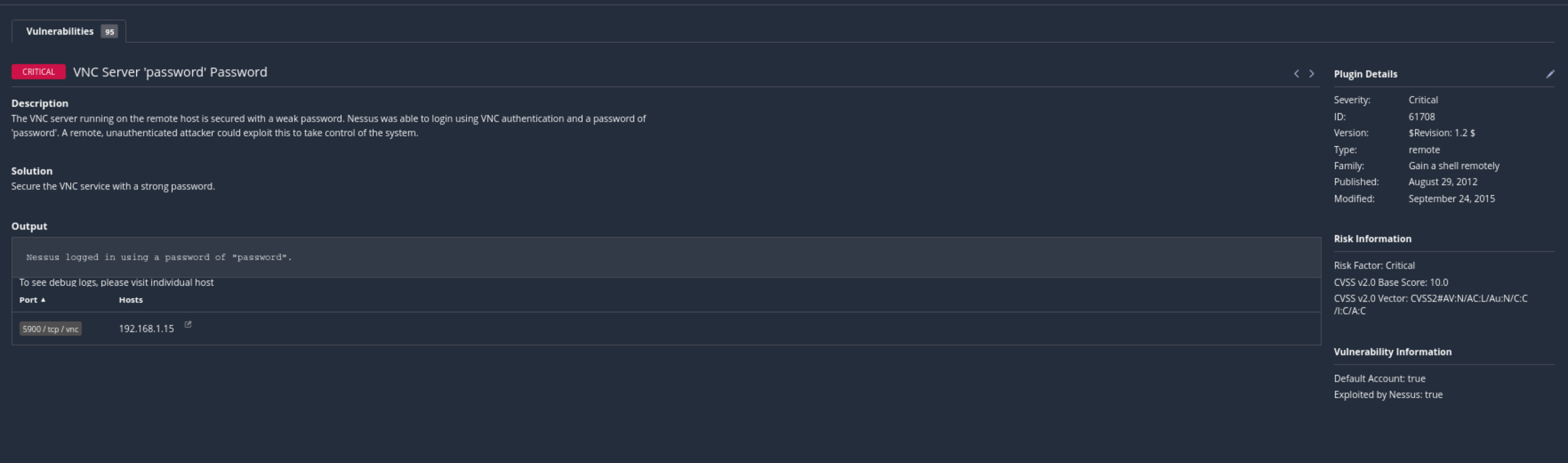
https://seclists.org/fulldisclosure/2010/Jun/277
https://seclists.org/fulldisclosure/2010/Jun/284
http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

Output

```
The remote IRC server is running as :

uid=0(root) gid=0(root)
```

To see debug logs, please visit individual host

Port ▲	Hosts
6667 / tcp / irc	192.168.1.15



CRITICAL VNC Server 'password' Password

Description
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution
Secure the VNC service with a strong password.

Output

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.1.15

Plugin Details

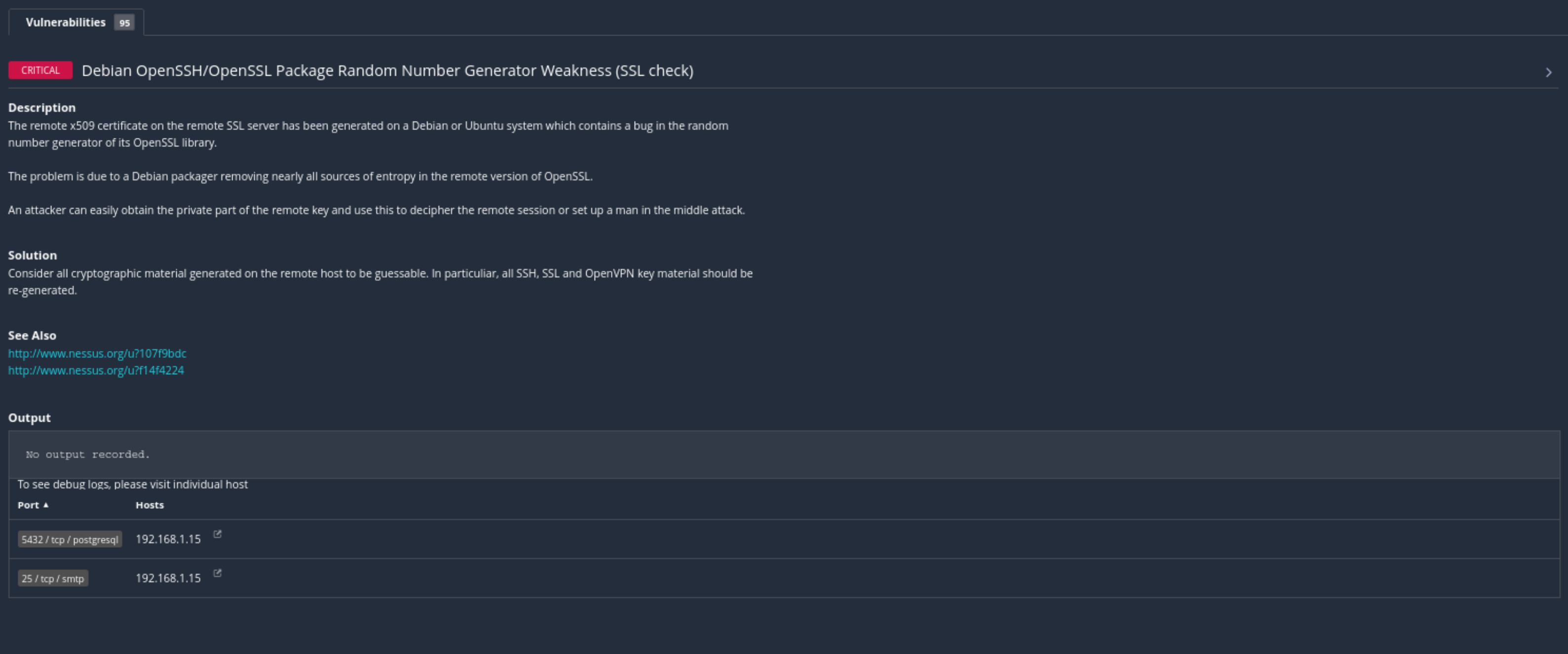
Severity:	Critical
ID:	61708
Version:	$Revision: 1.2 $
Type:	remote
Family:	Gain a shell remotely
Published:	August 29, 2012
Modified:	September 24, 2015

Risk Information

Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true
Exploited by Nessus: true



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

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.

Solution

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

See Also

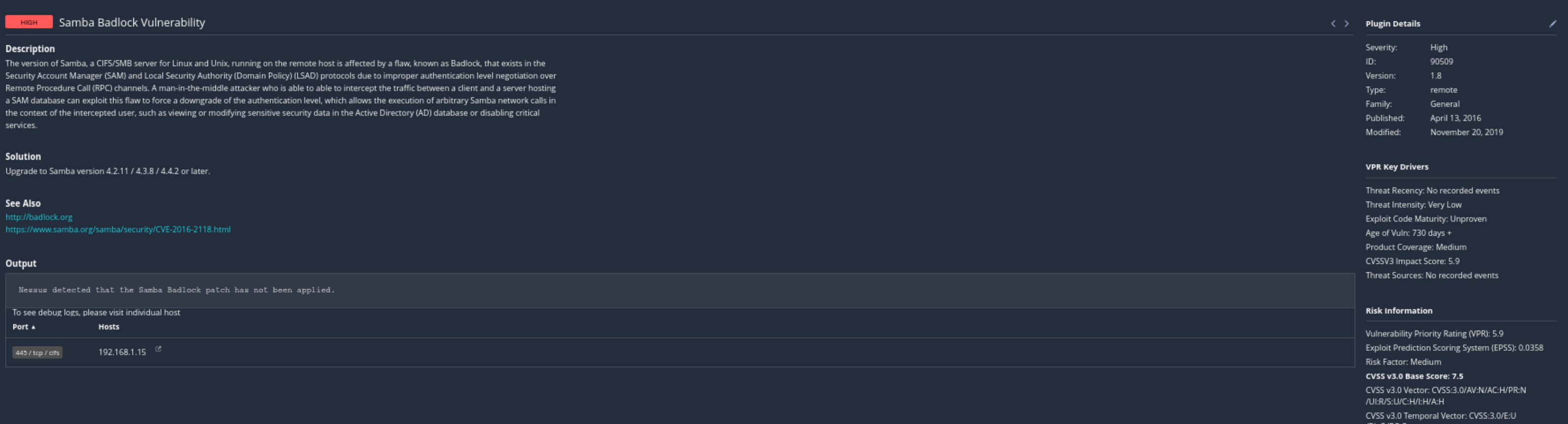
http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▲	Hosts
5432 / tcp / postgresql	192.168.1.15
25 / tcp / smtp	192.168.1.15



HIGH

Samba Badlock Vulnerability

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also

http://badlock.org
https://www.samba.org/samba/security/CVE-2016-2118.html

Output

```
Nessus detected that the Samba Badlock patch has not been applied.
```

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.1.15

Plugin Details

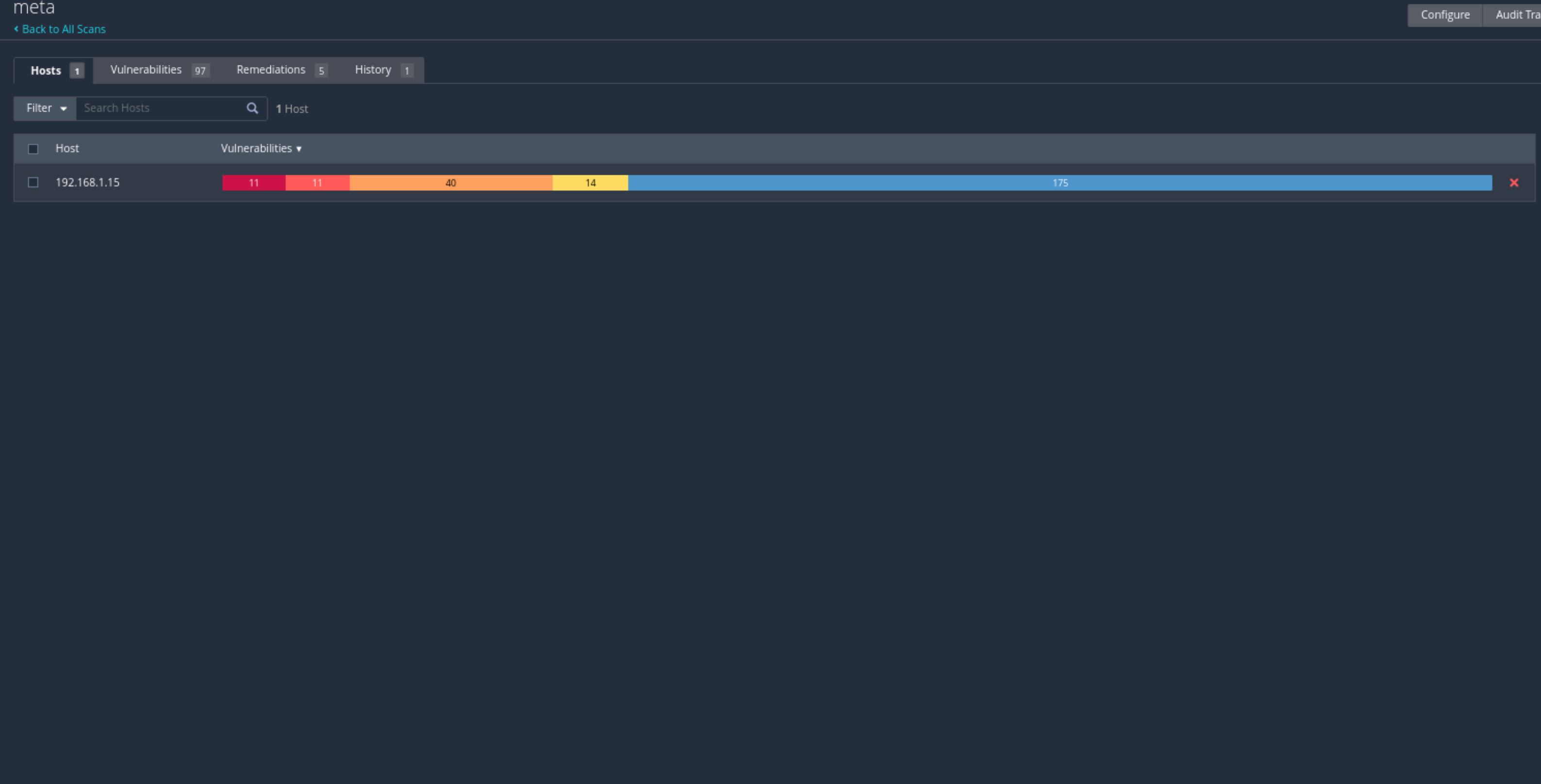
Severity: High
ID: 90509
Version: 1.8
Type: remote
Family: General
Published: April 13, 2016
Modified: November 20, 2019

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Medium
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

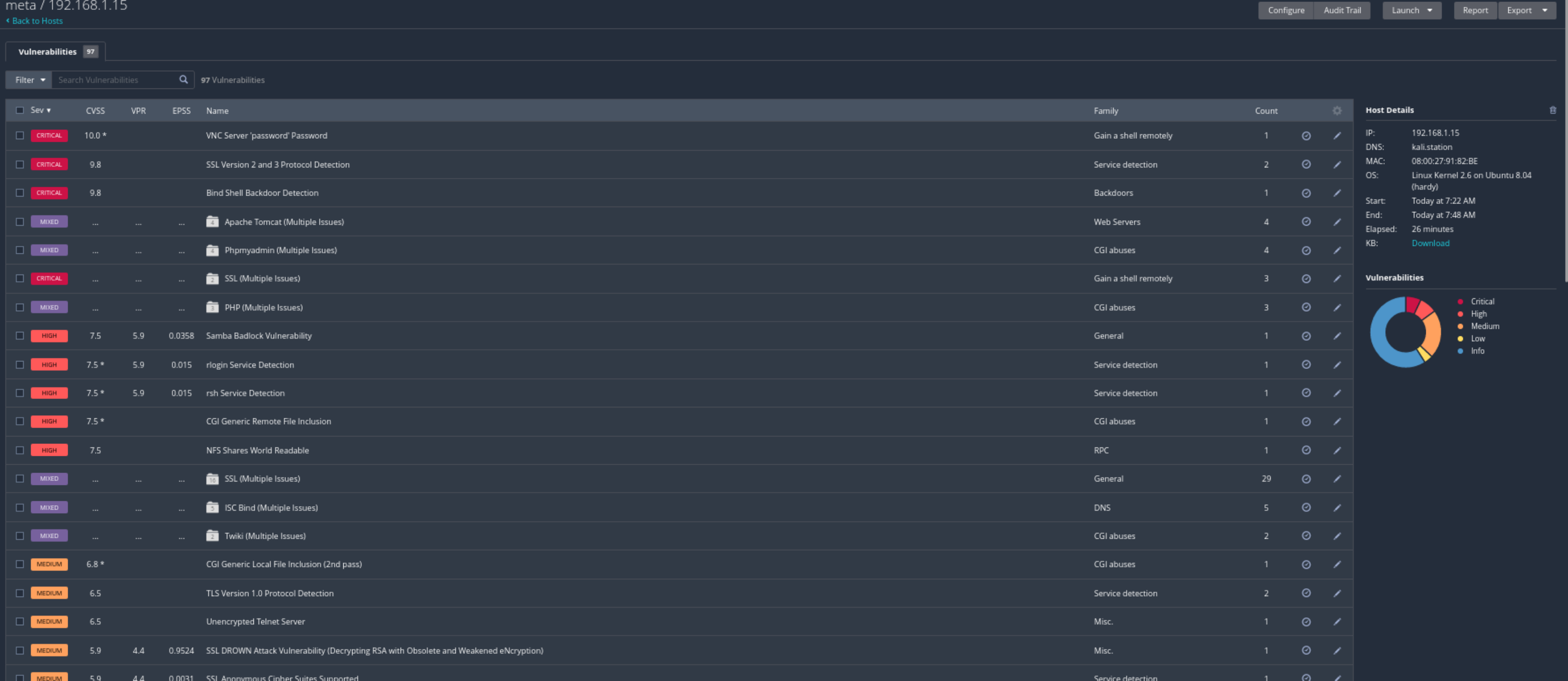
Vulnerability Priority Rating (VPR): 5.9
Exploit Prediction Scoring System (EPSS): 0.0358
Risk Factor: Medium
CVSS v3.0 Base Score: 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N /UI:R/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U



meta

1 Host

□	Host	Vulnerabilities ▾					
□	192.168.1.15	11	11	40	14	175	✕



meta / 192.168.1.15

‹ Back to Hosts

Vulnerabilities 97

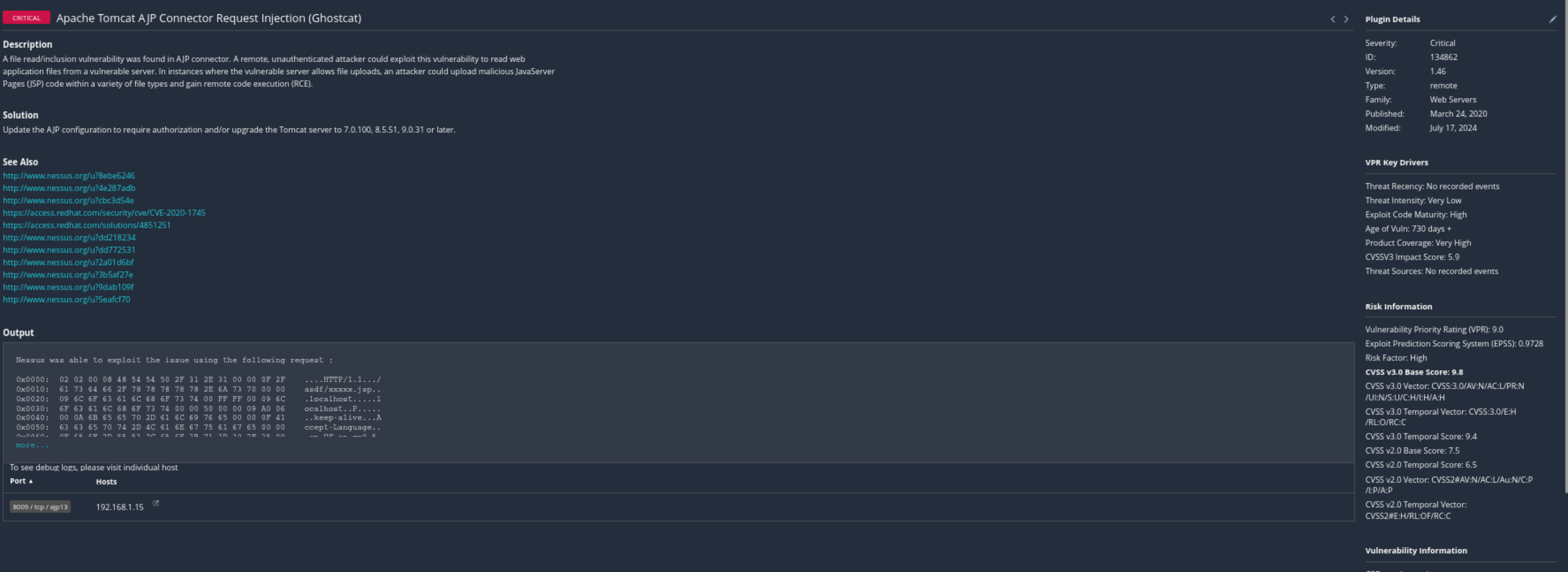
97 Vulnerabilities

□	Sev ▾	CVSS	VPR	EPSS	Name	Family	Count
□	CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
□	CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
□	CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
□	MIXED	...	...	...	4 Apache Tomcat (Multiple Issues)	Web Servers	4
□	MIXED	...	...	...	4 Phpmyadmin (Multiple Issues)	CGI abuses	4
□	CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
□	MIXED	...	...	...	3 PHP (Multiple Issues)	CGI abuses	3
□	HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1
□	HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1
□	HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1
□	HIGH	7.5 *			CGI Generic Remote File Inclusion	CGI abuses	1
□	HIGH	7.5			NFS Shares World Readable	RPC	1
□	MIXED	...	...	...	10 SSL (Multiple Issues)	General	29
□	MIXED	...	...	...	5 ISC Bind (Multiple Issues)	DNS	5
□	MIXED	...	...	...	2 Twiki (Multiple Issues)	CGI abuses	2
□	MEDIUM	6.8 *			CGI Generic Local File Inclusion (2nd pass)	CGI abuses	1
□	MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
□	MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
□	MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
□	MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	1

Host Details

IP: 192.168.1.15
DNS: kali.station
MAC: 08:00:27:91:82:BE
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 7:22 AM
End: Today at 7:48 AM
Elapsed: 26 minutes
KB: Download

Vulnerabilities



Apache Tomcat AJP Connector Request Injection (Ghostcat)

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.

See Also

http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
https://access.redhat.com/security/cve/CVE-2020-1745
https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234
http://www.nessus.org/u?dd772531
http://www.nessus.org/u?2a01d6bf
http://www.nessus.org/u?3b5af27e
http://www.nessus.org/u?9dab109f
http://www.nessus.org/u?5eafcf70

Output

```
Nessus was able to exploit the issue using the following request :

0x0000:  02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F    ....HTTP/1.1.../
0x0010:  61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00    asdf/xxxxx.jsp..
0x0020:  09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C    .localhost.....l
0x0030:  6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06    ocalhost..P.....
0x0040:  00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41    ..keep-alive...A
0x0050:  63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00    ccept-Language..
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
8009 / tcp / ajp13	192.168.1.15

Plugin Details

Severity: Critical
ID: 134862
Version: 1.46
Type: remote
Family: Web Servers
Published: March 24, 2020
Modified: July 17, 2024

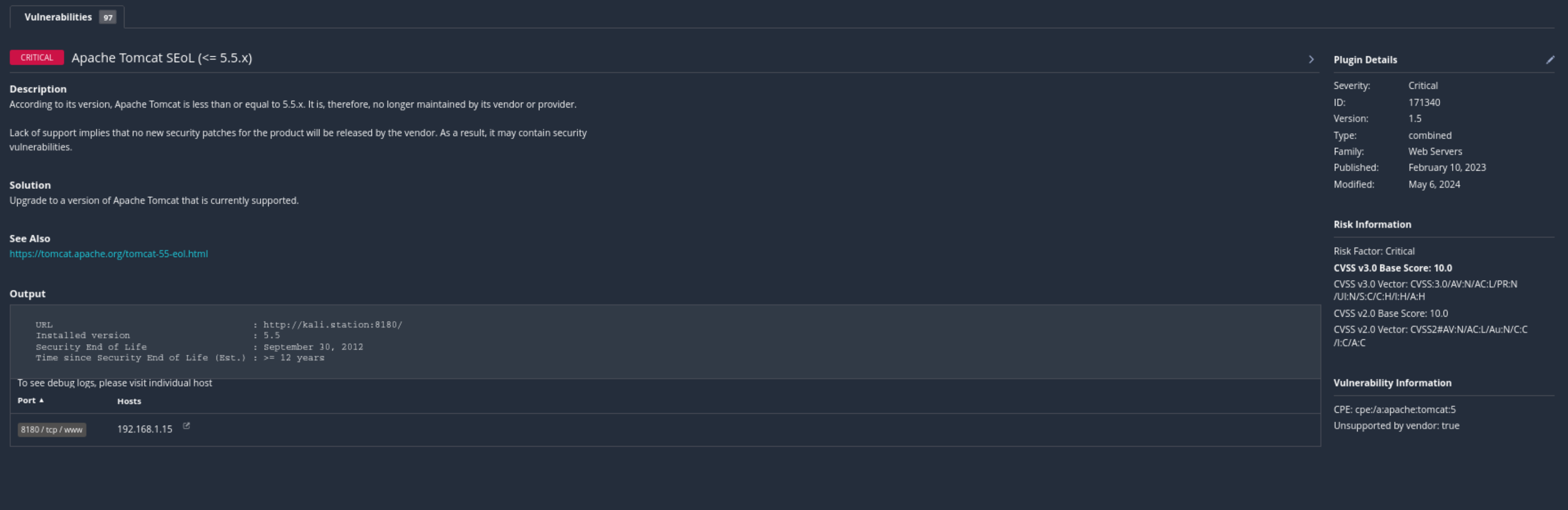
VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: High
Age of Vuln: 730 days +
Product Coverage: Very High
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 9.0
Exploit Prediction Scoring System (EPSS): 0.9728
Risk Factor: High
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.4
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Temporal Score: 6.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C

Vulnerability Information



CRITICAL Apache Tomcat SEoL (<= 5.5.x)

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.

See Also

https://tomcat.apache.org/tomcat-55-eol.html

Output

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

To see debug logs, please visit individual host

Port ▲	Hosts
8180 / tcp / www	192.168.1.15

Plugin Details

Severity:	Critical
ID:	171340
Version:	1.5
Type:	combined
Family:	Web Servers
Published:	February 10, 2023
Modified:	May 6, 2024

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score: 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

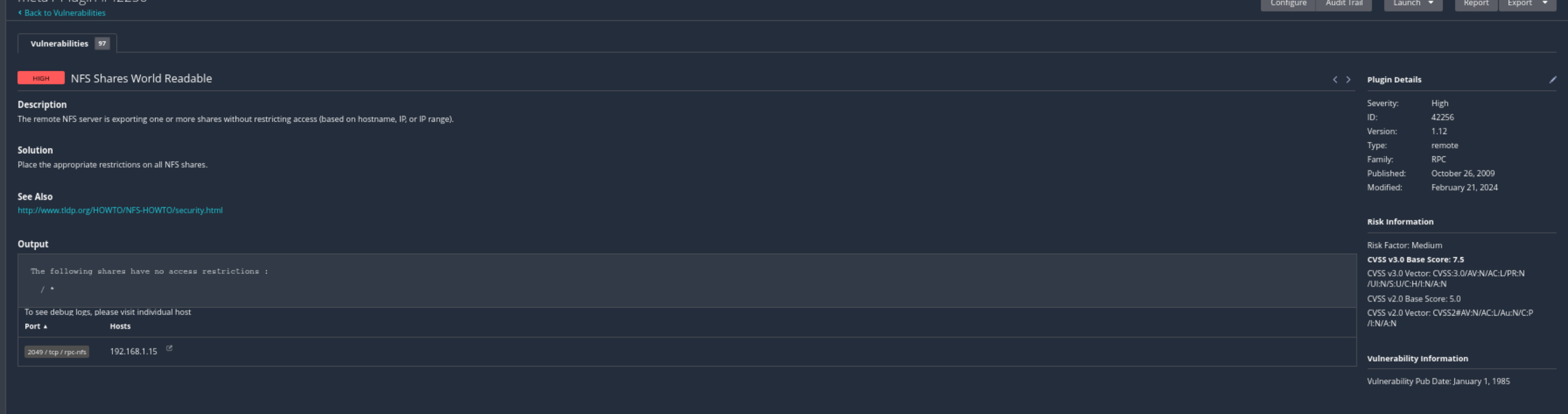
CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE: cpe:/a:apache:tomcat:5

Unsupported by vendor: true



NFS Shares World Readable

Description

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

Solution

Place the appropriate restrictions on all NFS shares.

See Also

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

Output

```
The following shares have no access restrictions :

  / *
```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / tcp / rpc-nfs	192.168.1.15

Plugin Details

Severity:	High
ID:	42256
Version:	1.12
Type:	remote
Family:	RPC
Published:	October 26, 2009
Modified:	February 21, 2024

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score: 7.5

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Information

Vulnerability Pub Date: January 1, 1985

meta common ports only

Report generated by Tenable Nessus™ Wed, 30 Oct 2024 08:26:29 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.1.15

8	10	31	10	94
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 153

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9514	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	0.0101	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1175	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	7.4	0.6988	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.8	7.4	0.9634	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	0.0164	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability
HIGH	7.5*	-	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5*	9.0	0.9514	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	6.7	0.0292	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary Code Injection (PMASA-2009-4)
HIGH	7.5*	5.9	0.015	10205	rlogin Service Detection

HIGH	7.5*	5.9	0.015	10245	rsh Service Detection
MEDIUM	6.5	3.6	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	0.9722	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.0031	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	0.9524	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet and Weakened eNcryption)
MEDIUM	5.9	4.4	0.0076	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	5.3	-	-	39467	CGI Generic Path Traversal
MEDIUM	5.3	4.0	0.0058	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	5.3	-	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0*	-	-	11411	Backup Files Disclosure
MEDIUM	4.3*	-	-	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3*	-	-	49067	CGI Generic HTML Injections (quick test)
MEDIUM	6.8*	-	-	42872	CGI Generic Local File Inclusion (2nd pass)
MEDIUM	4.3*	-	-	39466	CGI Generic XSS (quick test)
MEDIUM	5.0*	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.0*	7.3	0.0114	52611	SMTP Service STARTTLS Plaintext Command Injection

MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	0.9488	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FRE
MEDIUM	5.0*	-	-	57640	Web Application Information Disclosure
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3*	3.8	0.0102	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	5.0*	-	-	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-200
MEDIUM	4.3*	3.0	0.0022	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-20
LOW	3.7	3.6	0.6115	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	0.9736	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	3.9	0.9736	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam)
LOW	3.4	5.1	0.9749	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	-	26194	Web Server Transmits Cleartext Credentials
LOW	2.6*	-	-	10407	X Server Detection
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	46180	Additional DNS Hostnames
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)

INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	72779	DNS Server Version Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11156	IRC Daemon Version Detection
INFO	N/A	-	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosur
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remo check)
INFO	N/A	-	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

INFO	N/A	-	-	50345	Missing or Permissive X-Frame-Options HTTP Response Heade
INFO	N/A	-	-	10437	NFS Share Export List
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	22227	RMI Registry Detection
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information

INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	62563	SSL Compression Methods Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	25240	Samba Server Detection
INFO	N/A	-	-	104887	Samba Version
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	14773	Service Detection: 3 ASCII Digit Code Responses
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
INFO	N/A	-	-	19941	TWiki Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10281	Telnet Server Detection
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	19288	VNC Server Security Type Detection
INFO	N/A	-	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	-	10342	VNC Software Detection
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	100669	Web Application Cookies Are Expired

INFO	N/A	-	-	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	-	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	-	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	-	-	91815	Web Application Sitemap
INFO	N/A	-	-	11032	Web Server Directory Enumeration
INFO	N/A	-	-	49705	Web Server Harvested Email Addresses
INFO	N/A	-	-	11419	Web Server Office File Inventory
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	-	10662	Web mirroring
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	17219	phpMyAdmin Detection
INFO	N/A	-	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

meta

Report generated by Tenable Nessus™ Wed, 30 Oct 2024 07:48:51 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.1.15

9	10	33	11	98
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 161

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9514	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	0.0101	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1175	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.8	7.4	0.9634	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	0.0164	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability
HIGH	7.5*	-	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5*	9.0	0.9514	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	6.7	0.0292	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary Code Injection (PMASA-2009-4)

HIGH	7.5*	5.9	0.015	10205	rlogin Service Detection
HIGH	7.5*	5.9	0.015	10245	rsh Service Detection
MEDIUM	6.5	3.6	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	0.9722	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.0031	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	0.9524	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet and Weakened eNcryption)
MEDIUM	5.9	4.4	0.0076	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	5.3	-	-	39467	CGI Generic Path Traversal
MEDIUM	5.3	4.0	0.0058	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	5.3	2.2	0.2769	35806	Tomcat Sample App cal2.jsp 'time' Parameter XSS
MEDIUM	5.3	-	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0*	-	-	11411	Backup Files Disclosure
MEDIUM	4.3*	-	-	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3*	-	-	49067	CGI Generic HTML Injections (quick test)
MEDIUM	6.8*	-	-	42872	CGI Generic Local File Inclusion (2nd pass)

MEDIUM	4.3*	-	-	39466	CGI Generic XSS (quick test)
MEDIUM	5.0*	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.0*	7.3	0.0114	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	0.9488	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FRE
MEDIUM	5.0*	-	-	57640	Web Application Information Disclosure
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3*	3.8	0.0102	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	5.0*	-	-	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-200
MEDIUM	4.3*	3.0	0.0022	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-20
LOW	3.7	3.6	0.6115	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	0.9736	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	3.9	0.9736	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam)
LOW	3.4	5.1	0.9749	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	-	26194	Web Server Transmits Cleartext Credentials
LOW	2.6*	-	-	34850	Web Server Uses Basic Authentication Without HTTPS
LOW	2.6*	-	-	10407	X Server Detection
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	21186	AJP Connector Detection
INFO	N/A	-	-	46180	Additional DNS Hostnames

INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39446	Apache Tomcat Detection
INFO	N/A	-	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	72779	DNS Server Version Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11156	IRC Daemon Version Detection

INFO	N/A	-	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosur
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remo check)
INFO	N/A	-	-	50344	Missing or Permissive Content-Security-Policy frame-ancestor HTTP Response Header
INFO	N/A	-	-	50345	Missing or Permissive X-Frame-Options HTTP Response Heade
INFO	N/A	-	-	10437	NFS Share Export List
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	40665	Protected Web Page Detection
INFO	N/A	-	-	22227	RMI Registry Detection
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support

INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	62563	SSL Compression Methods Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	25240	Samba Server Detection
INFO	N/A	-	-	104887	Samba Version
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
INFO	N/A	-	-	19941	TWiki Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10281	Telnet Server Detection

INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	19288	VNC Server Security Type Detection
INFO	N/A	-	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	-	10342	VNC Software Detection
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	-	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	-	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	-	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	-	-	91815	Web Application Sitemap
INFO	N/A	-	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	11032	Web Server Directory Enumeration
INFO	N/A	-	-	49705	Web Server Harvested Email Addresses
INFO	N/A	-	-	11419	Web Server Office File Inventory
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	-	10662	Web mirroring
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	17219	phpMyAdmin Detection
INFO	N/A	-	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown