https://localhost:8834/#/scans/reports/23/vulnerabilities/group/171340

Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

ntials | Scans | Settings

metasploit scan / Apache Tomcat (Multiple Issues)

« Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | E

Hosts 1 | Vulnerabilities 69 | Remediations 2 | History 1

Search Vulnerabilities

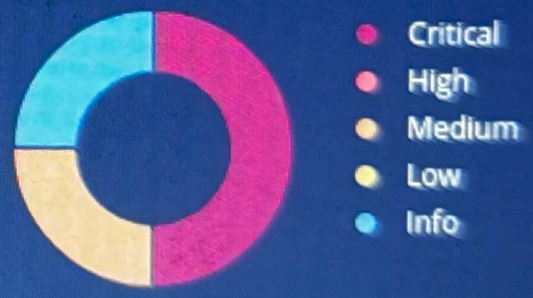
4 Vulnerabilities

Sev	CVSS	VPR	EPSS	N...	Family	Count
CRITICAL	10.0				ApacWeb Servers	1
CRITICAL	9.8	8.9	0.9447		ApacWeb Servers	1
MEDIUM	5.3				ApacWeb Servers	1
INFO					ApacWeb Servers	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 11:40 AM
End:	Today at 11:48 AM
Elapsed:	9 minutes

Vulnerabilities



metasploit scan / Plugin #83875

« Back to Vulnerabilities

Configure Audit Trail Launch Report Exp

Hosts 1 Vulnerabilities 69 Remediations 2 History 1

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

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.

Solution

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

See Also

https://weakdh.org/

Output

```
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
```

Plugin Details

Severity:	Low
ID:	83875
Version:	1.41
Type:	remote
Family:	Misc.
Published:	May 28, 2015
Modified:	September 11, 2024

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 730 days +

Product Coverage: Very High

CVSSV3 Impact Score: 1.4

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 4.5

https://localhost:8834/#/scans/reports/23/vulnerabilities/10205

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

sentials Scans Settings

Hosts 1 | Vulnerabilities 69 | Remediations 2 | History 1

HIGH **rlogin Service Detection**

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.
Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▲	Hosts
513 / tcp / rlogin	192.168.1.100

Plugin Details

Severity:	High
ID:	10205
Version:	1.36
Type:	remote
Family:	Service detection
Published:	August 30, 1999
Modified:	April 11, 2022

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): 7.4
Exploit Prediction Scoring System (EPSS): 0.46
Risk Factor: High

https://localhost:8834/#/scans/reports/23/vulnerabilities/201352

Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

s Essentials | Scans | Settings

nuray

Hosts 1 | Vulnerabilities 69 | Remediations 2 | History 1

CRITICAL **Canonical Ubuntu Linux SEoL (8.04.x)**

Description

According to its version, Canonical Ubuntu Linux is 8.04.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 Canonical Ubuntu Linux that is currently supported.

See Also

http://www.nessus.org/u?3bdb2d2e

Output

```
OS                                    : Ubuntu Linux 8.04
Security End of Life                  : May 9, 2013
Time since Security End of Life (Est.) : >= 11 years
```

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	192.168.1.100

Plugin Details

Severity:	Critical
ID:	201352
Version:	1.2
Type:	combined
Family:	General
Published:	July 3, 2024
Modified:	March 26, 2025

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:/o:canonical:ubuntu_linux

Unsupported by vendor: true

Right Ctrl

ünüm Giriş Aygıtlar Yardım

es

May 6 12:15 PM

1% 21% 0.0 kB 0.0 kB

ıtials / Folde ×

https://localhost:8834/#/scans/reports/23/hosts

ools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Essentials Scans Settings

nuray

metasploit scan

« Back to My Scans

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | Vulnerabilities 69 | Remediations 2 | History 1

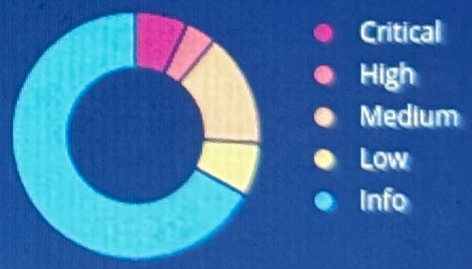
Filter | Search Hosts | 1 Host

Host	Vulnerabilities
192.168.1.100	10 6 24 9 136

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 11:40 AM
End:	Today at 11:48 AM
Elapsed:	9 minutes

Vulnerabilities



Right Ctrl