

Vulnerabilities

Total: 108

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

1.

33850 - Unix Operating System Unsupported Version Detection

Synopsis

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

Description

According to its self-reported 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)

```
msfadmin@metasploitable:~$ sudo apt update
sudo: apt: command not found
msfadmin@metasploitable:~$ sudo apt-get update
```

Ho aggiornato il sistema e il problema si è risolto.

2.

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak 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.

Risk Factor

Critical

CVSS v2.0 Base Score

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

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
Passwords do not match. Please try again.

Password:
Verify:
msfadmin@metasploitable:~$
```

Ho modificato la password.

3.

11356 - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

```
% /etc/exports: the access control list for filesystems which may be exported
%                to NFS clients.  See exports(5).
%
% Example for NFSv2 and NFSv3:
% /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
%
% Example for NFSv4:
% /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
% /srv/nfs4/homes gss/krb5i(rw,sync)
%
% path/to/share 192.168.50.101 (rw,sync,no_subtree_check)
```

Ho aperto il file `/etc/exports` con un editor di testo. Questo file contiene le configurazioni delle condivisioni NFS. Ho aggiunto le righe necessarie per specificare le condivisioni e gli host autorizzati.

4.

Vulnerabilities

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).

See Also

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

```
tar -xvf apache-tomcat-9.0.31.tar.gz -C /path/to/
```

```
/path/to/new-tomcat/bin/startup.sh
```

Ho rimosso la vecchia installazione di Tomcat installato quella nuova.