



RIMEDIALLE

VULNERABILITÀ



Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)**51988 - Bind Shell Backdoor Detection****32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness****32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)****32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)****11356 - NFS Exported Share Information Disclosure****20007 - SSL Version 2 and 3 Protocol Detection****20007 - SSL Version 2 and 3 Protocol Detection****33850 - Unix Operating System Unsupported Version Detection****61708 - VNC Server 'password' Password****26760 - ISC BIND Service Denial of Service / Reflected DoS**

Dopo un'analisi approfondita di Metasploitable con Nessus, sono state individuate 10 vulnerabilità critiche. Ho deciso di concentrarmi sulla risoluzione delle 4 più gravi.

[Download report](#)[Learn More](#)

02

Prima di iniziare, è essenziale stabilire un processo sistematico:

- 1. Identificare le Vulnerabilità:** Verificare un elenco dettagliato delle vulnerabilità, comprese le modalità di sfruttamento.
- 2. Priorizzare le Risoluzioni:** Iniziare con le vulnerabilità più critiche.
- 3. Ricerca di Patch o Mitigazioni:** Trovare patch di sicurezza o metodi di mitigazione raccomandati per ogni vulnerabilità.
- 4. Applicare le Soluzioni:** Applicare le patch o le mitigazioni identificate, seguendo le migliori pratiche per ridurre al minimo l'impatto sul sistema.
- 5. Verifica e Test:** Eseguire nuovamente la scansione con Nessus dopo l'applicazione delle soluzioni per assicurarsi che le vulnerabilità siano state risolte.





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

<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?5eacf70>

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.

APACHE TOMCAT AJP

La prima vulnerabilità riguardava il server Apache Tomcat 7.X o versioni inferiori, soggette a una vulnerabilità che consente a un utente esterno di leggere i file presenti.

Learn More

04



Come prima cosa ho controllato la versione di Tomcat scaricata sul mio sistema

```
msfadmin@metasploitable:~$ dpkg -l | grep tomcat
ii  libtomcat5.5-java
    Java Servlet engine -- core libraries
ii  tomcat5.5
    Servlet and JSP engine
ii  tomcat5.5-admin
    Java Servlet engine -- admin & manager web interface
ii  tomcat5.5-webapps
    Java Servlet engine -- documentation and examples
msfadmin@metasploitable:~$
```

```
root@metasploitable:~# mkdir /tmp/tomcat_backup
root@metasploitable:~# cp -r /var/lib/tomcat5.5/conf /var/lib/tomcat5.5/work /tmp/tomcat_backup
root@metasploitable:~# ls /tmp/tomcat_backup
conf  work
root@metasploitable:~# ls /tmp/tomcat_backup/conf
Catalina          context.xml        server-minimal.xml  tomcat-users.xml
catalina.policy   logging.properties  server.xml        web.xml
catalina.properties  policy.d        tomcat5.5
root@metasploitable:~# ls /tmp/tomcat_backup/work
/tmp/tomcat_backup/work
root@metasploitable:~# _
```

Poi ho effettuato un backup dei file più importanti, conf e work, perchè Tomcat non può essere aggiornato direttamente dal terminale ma deve essere reinstallato manualmente.



Poi ho provato a scaricare la nuova versione di Tomcat da internet e salvarla nella cartella tmp con il comando:

`wget`

`https://downloads.apache.org/tomcat/tomcat-11/v11.0.0-M20/bin/apache-tomcat-11.0.0-M20.tar.gz -P /tmp`

ma ho avuto dei problemi e dopo diversi tentativi ho deciso di aggirarlo scaricando il file su un altro computer appartenente alla stessa rete di Metasploitable

Index of /tomcat/tomcat-11/v11.0.0-M20/bin

Name	Last modified	Size	Description
Parent Directory		-	
embed/	2024-05-08 09:24	-	
apache-tomcat-11.0.0-M20-deployer.tar.gz	2024-05-03 16:08	3.0M	
apache-tomcat-11.0.0-M20-deployer.tar.gz.asc	2024-05-03 16:08	849	
apache-tomcat-11.0.0-M20-deployer.tar.gz.sha512	2024-05-03 16:08	170	
apache-tomcat-11.0.0-M20-deployer.zip	2024-05-03 16:08	3.0M	
apache-tomcat-11.0.0-M20-deployer.zip.asc	2024-05-03 16:08	849	
apache-tomcat-11.0.0-M20-deployer.zip.sha512	2024-05-03 16:08	167	
apache-tomcat-11.0.0-M20-fulldocs.tar.gz	2024-05-03 16:08	7.1M	
apache-tomcat-11.0.0-M20-fulldocs.tar.gz.asc	2024-05-03 16:08	849	
apache-tomcat-11.0.0-M20-fulldocs.tar.gz.sha512	2024-05-03 16:08	170	
apache-tomcat-11.0.0-M20-windows-x64.zip	2024-05-03 16:08	14M	
apache-tomcat-11.0.0-M20-windows-x64.zip.asc	2024-05-03 16:08	849	
apache-tomcat-11.0.0-M20-windows-x64.zip.sha512	2024-05-03 16:08	170	
apache-tomcat-11.0.0-M20.exe	2024-05-03 16:08	13M	
apache-tomcat-11.0.0-M20.exe.asc	2024-05-03 16:08	849	
apache-tomcat-11.0.0-M20.exe.sha512	2024-05-03 16:08	158	
apache-tomcat-11.0.0-M20.tar.gz	2024-05-03 16:08	12M	
apache-tomcat-11.0.0-M20.tar.gz.asc	2024-05-03 16:08	849	
apache-tomcat-11.0.0-M20.tar.gz.sha512	2024-05-03 16:08	161	
apache-tomcat-11.0.0-M20.zip	2024-05-03 16:08	13M	
apache-tomcat-11.0.0-M20.zip.asc	2024-05-03 16:08	849	
apache-tomcat-11.0.0-M20.zip.sha512	2024-05-03 16:08	158	



e di trasferire il file su Metasploitable con il comando

```
(kali㉿kali)-[~/Downloads]
$ scp -oHostKeyAlgorithms=+ssh-rsa apache-tomcat-11.0.0-M20.tar.gz msfadmin@192.168.50.2:/tmp
The authenticity of host '192.168.50.2 (192.168.50.2)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.2' (RSA) to the list of known hosts.
msfadmin@192.168.50.2's password:
apache-tomcat-11.0.0-M20.tar.gz
```

```
root@metasploitable:~# tar -x -z -f /tmp/apache-tomcat-11.0.0-M20.tar.gz -C /var
/lib
root@metasploitable:~# cd /var/lib
root@metasploitable:/var/lib# ls
apache-tomcat-11.0.0-M20  gcj-4.2          mysql           sgml-base
apparmor                  gconf             mysql-cluster   tomcat5.5
apt                      initramfs-tools  nfs              ucf
aptitude                 initscripts       postfix         update-manager
beelocs                  libuuid           postgresql     urandom
bind                     locales           python-support vim
defoma                   logrotate        python-support samba
dhcpc3                   misc              security      x11
dpkg                     mlocate          security      xkb
root@metasploitable:/var/lib# mv apache-tomcat-11.0.0-M20 tomcat11
root@metasploitable:/var/lib#
```

poi ho estratto il file tar nella directory /var/lib e l'ho rinominata in tomcat11



e ho sovrascritto i file di backup che avevo fatto in precedenza

```
root@metasploitable:~# mv -i /tmp/tomcat/conf /var/lib/tomcat11
root@metasploitable:~# mv -i /tmp/tomcat/webapps /var/lib/tomcat11
```

```
root@metasploitable:/var/lib# ./tomcat11/bin/startup.sh
Using CATALINA_BASE:  /var/lib/tomcat11
Using CATALINA_HOME:  /var/lib/tomcat11
Using CATALINA_TMPDIR: /var/lib/tomcat11/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /var/lib/tomcat11/bin/bootstrap.jar:/var/lib/tomcat11/bin
/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
root@metasploitable:/var/lib#
```

ed infine ho provato ad avviare Tomcat



51988 - Rilevamento backdoor shell di associazione

Sinossi
L'host remoto potrebbe essere stato compromesso.

Descrizione
Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla connettendosi alla porta remota e inviando direttamente i comandi.

Soluzione
Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

Fattore di rischio
Critico

Punteggio di base CVSS v3.0
9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Punteggio di base CVSS v2.0
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Informazioni sul plug-in
Pubblicato: 15/02/2011, modificato: 11/04/2022

Uscita plug-in
TCP/1524/wild_shell

BACKDOOR

La seconda vulnerabilità è una backdoor installata sulla porta TCP 1524 e da questa una persona esterna può avere accesso al computer e poi spostarsi all'interno della rete



Come prima cosa ho usato questo comando per mostrare le connessioni di rete aperte sulla porta 1524, inclusi i dettagli come il protocollo utilizzato, il PID del processo che ha aperto la connessione e il nome del processo.

```
root@metasploitable:~# lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4452 root    12u  IPv4  12059      TCP *:ingreslock (LISTEN)
root@metasploitable:~# _
```

```
root@metasploitable:/etc/xinetd.d# ls
chargen  daytime  discard  echo  time  vsftpd
```

Poi sono andato ad analizzare i file nella cartella del processo in esecuzione sulla porta, ma non ho trovato nulla di sospetto



Ho analizzato il processo
xinetd e ho visto che è attivo
nella directory /usr/sbin/xinetd
ed ho eliminato i file dentro
questa cartella

```
root@metasploitable:/etc/xinetd.d# ps aux | grep xinetd
root      4452  0.0  0.0  2424   856 ?        Ss   03:58   0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
root      4917  0.0  0.0  3004   752 tty1     R+   04:58   0:00 grep xinetd
```

```
root@metasploitable:/usr/sbin# kill 4452
root@metasploitable:/usr/sbin# lsof -i :1524
root@metasploitable:/usr/sbin#
root@metasploitable:/usr/sbin# ps aux | grep xinetd
root      5007  0.0  0.0  3004   756 tty1     R+   05:17   0:00 grep xinetd
root@metasploitable:/usr/sbin# _
```

infine ho arrestato il processo
indicando il PID ed ho provato a
vedere se era ancora attivo nella
porta



11356 - Divulgazione di informazioni sulle azioni esportate NFS

Sinossi
È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione
Almeno una delle condivisioni NFS esportate dal server remoto può essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questa funzionalità per leggere (ed eventualmente scrivere) file su un host remoto.

Soluzione
Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le condivisioni remote.

Fattore di rischio
Critico

Punteggio VPR
5.9

Punteggio di base CVSS v2.0
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Referenze

CVE	CVE-1999-0170
CVE	Codice CVE-1999-0211
CVE	Codice CVE-1999-0554

Sfruttabile con
Metasploit (vero)

Informazioni sul plug-in

Pubblicato: 2003/03/12, modificato: 2023/08/30

NFS SHARES

La terza vulnerabilità riguarda la condivisione dei file attraverso NFS, qualsiasi utente ha la possibilità di accedere a qualsiasi cartella attraverso NFS e leggere e scrive file

[Learn More](#)

12



Sono andato subito a controllare le impostazioni all'interno del seguente file

root@metasploitable:~# nano /etc/exports

```
GNU nano 2.0.7          File: /etc/exports          Modified

# /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)
#
# *(rw,sync,no_root_squash,no_subtree_check)
```

qui la condivisione è abilitata per qualsiasi ip con "*" ed ha accesso a qualsiasi cartella del sistema "/"



Ho impostato la seguente regola per regolare li accessi e permettere l'accesso soltanto agli utenti con quel'indirizzo IP

```
GNU nano 2.0.7           File: /etc/exports           Modified

# /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)
#
#   192.168.50.100(rw,sync,no_root_squash,no_subtree_check)
```



61708 - Password 'password' server VNC

-

Sinossi

Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

Descrizione

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di 'password'. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

Soluzione

Proteggi il servizio VNC con una password complessa.

Fattore di rischio

Critico

Punteggio di base CVSS v2.0

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

Informazioni sul plug-in

Pubblicato: 2012/08/29, Modificato: 2015/09/24

Uscita plug-in

TCP/5900/VNC

Nessus ha effettuato l'accesso utilizzando una password di "password".

SERVER VNC

La quarta vulnerabilità riguarda il server VNC con il quale si accede ad un desktop remoto ed è possibile leggere e scrivere e eseguire su tutto il sistema.
Il server è protetto da un password debole “password” che è facile da scoprire con un semplice attacco Brute Force con dizionario



La prima cosa che ho fatto è stata quella di vedere il processo in esecuzione sulla porta 5900, la porta che Nessus ha rilevato in cui è attivo il server e poi ho cercato come modificare la password per Xtightvnc, ho impostato una password sicura ed ho riavviato il server.

```
msfadmin@metasploitable:~$ sudo lsof -i :5900
COMMAND   PID USER   FD   TYPE DEVICE SIZE NODE NAME
xtightvnc 4576 root    3u  IPv4  12237      TCP *:5900 (LISTEN)
msfadmin@metasploitable:~$ sudo kill 4576
msfadmin@metasploitable:~$ sudo lsof -i :590
msfadmin@metasploitable:~$ sudo lsof -i :5900
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$ vncserver
xauth:  creating new authority file /home/msfadmin/.Xauthority
New 'X' desktop is metasploitable:1

Creating default startup script /home/msfadmin/.vnc/xstartup
Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log
```

Dopo aver affrontato queste vulnerabilità, ho rieseguito la scansione e ho verificato che le vulnerabilità fossero state correttamente risolte. Tuttavia, è stata rilevata una nuova backdoor attraverso una versione corrotta di UnrealIRCd. Per ridurre ulteriormente il rischio, sarà necessario eliminare o ridurre al minimo le altre vulnerabilità con il tempo.

192.168.50.101

7	4	24	11	124
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Sat May 11 09:56:57 2024
End time: Sat May 11 10:05:51 2024

Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.50.101
MAC Address: 08:00:27:A8:0F:D4
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

[32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness](#) +
[32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness \(SSL check\)](#) +
[32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness \(SSL check\)](#) +
[20007 - SSL Version 2 and 3 Protocol Detection](#) +
[20007 - SSL Version 2 and 3 Protocol Detection](#) +
[33850 - Unix Operating System Unsupported Version Detection](#) +
[46882 - UnrealIRCd Backdoor Detection](#) +

[Download report](#)[Learn More](#)



THANK YOU