

NESSUS

vulnerability assessment

ARGOMENTI TRATTATI

RIASSUNTO

VULNERABILITA 1 -4 PAGINA

VULNERABILITA 2 -7 PAGINA

VULNERABILITA 3 -8 PAGINA

VULNERABILITA 4 -9 PAGINA

INDICE

RIASSUNTO - TRACCIA

Nell'esercizio di oggi dobbiamo scansionare la macchina virtuale metasploitable con il programma Nessus, trovando problemi critici e aggiustarli.

Metasploitable è una macchina virtuale in cui è implementato una grande quantità di vulnerabilità per lo scopo educativo, per questo è ideale utilizzarlo in questo progetto.

Dopo di avere acceso la macchina metasploitable e kali, si attiva Nessus, in cui troverai l'immagine affianco, da qui potrai vedere tutte le vulnerabilità che il network ne ha. Scegliendo 4 vulnerabilità critiche andremmo ad aggiustarla.

Vulnerabilities				
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	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

Total: 149

PRIMA VULNERABILITÀ

VULNERABILITÀ 1: NFS EXPORTED SHARE INFORMATION DISCLOSURE

Questa vulnerabilità è critica dovuto al fatto che chiunque possa connettersi tramite una NFS di Meta, quindi potrebbe scrivere o leggere archivi che siano sensibili.

CRITICAL NFS Exported Share Information Disclosure >

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.

PRIMA VULNERABILITÀ

VULNERABILITÀ 1: NFS EXPORTED SHARE INFORMATION DISCLOSURE

La soluzione per tale problema è individuare la cartella impostazione file dei NFS, vedere quali permessi hanno i Host del server. Al suo interno si nota che tutti i IP (*) hanno il permesso per modificare e accedere a qualsiasi directory della metà.

```
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)
```

PRIMA VULNERABILITÀ

VULNERABILITÀ 1: NFS EXPORTED SHARE INFORMATION DISCLOSURE

Modificando il file per solo il server avere tutti i permessi solve il problema a riguardo gli NFS. Questo garantisce che sia richiesto dal server stesso per modificare un file che potrebbe essere un backup.

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

PRIMA VULNERABILITÀ

VULNERABILITÀ 2: APACHE TOMCAT AJP

Questa vulnerabilità è dovuta al fatto che un programma non sia attualizzato, garantendo che un utente di leggere gli archivi interni al server.

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

PRIMA VULNERABILITÀ

VULNERABILITÀ 3: PASSWORD “PASSWORD”

Questa vulnerabilità è dovuta dal fatto che la password scelta per l'admin è “password” che è molto facile da scoprire tramite un brute force, quindi basta modificare la password del host per qualcosa più adeguato.

```
msfadmin@metasploitable:~$ uncpassword
Using password file /home/msfadmin/.unc/password
Password:
Verify:
```

PRIMA VULNERABILITÀ

VULNERABILITÀ 4: APACHE TOMCAT AJP

La soluzione più semplice è attualizzare il programma Tomcat e vedere se la vulnerabilità sia ancora aperta alla fine con un scan di Nessus. Dovuta alla precaria stabilità di metà, il metodo più facile è stato trasferire il file direttamente da un utente al host, invece di conneterlo con una scheda con una rete esterna.

```
(kali㉿kali)-[~/Downloads]
$ scp -oHostKeyAlgorithms=+ssh-rsa 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
```

estraendo il file sembra che abbia sostituito e aggiustato il file,
perchè non è stato rivelato da Nessus dopo.