

Report S5L4

Per questo Report prenderemo in considerazione le criticità di livello critico riscontrate dallo scan di Nessus sulla macchina metasploitable.

192.168.1.188



Vulnerabilities

Total: 100

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	-	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*	-	61708	VNC Server 'password' Password

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Una vulnerabilità di lettura/inclusione di file è stata trovata nel connettore AJP. Un attaccante remoto, non autenticato, potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile permette il caricamento di file, un attaccante potrebbe caricare codice JSP (JavaServer Pages) malevolo all'interno di vari tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Per mitigare la vulnerabilità nel connettore AJP di Apache Tomcat, è necessario aggiornare la configurazione di AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat alle versioni 7.0.100, 8.5.51, 9.0.31 o successive.

Bind Shell Backdoor Detection

Una shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un attaccante può utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

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	192.168.1.188 

Come possiamo osservare Nessus ha rilevato una backdoor per la metasploit, interessante è vedere che a fondo pagina ci illustra I comandi usati e parte dei risultati ottenuti.

VNC Server 'password' Password

Come evidenziato il server remoto VNC della meta, ha impostato come password:“password”, il che può permettere a chiunque di entrare nel VNC e prendere controllo del sistema da remoto.

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	192.168.1.188 

Il VNC è molto delicato e va protetto con una password forte.