Metasploitable Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1
HIGH	7.5		NFS Shares World Readable	RPC	1

1) *Critical:* NFS Exported Share information Disclosure.

(L'NFS consente la condivisione remota dei dati a livello di file. Un utente (o un dispositivo client) può utilizzare NFS per connettersi a un server di rete e accedere ai file presenti sul server. Più macchine client (utenti) possono condividere lo stesso file senza conflitti di dati.) Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice in modalità remota (RCE).

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

2) *Critical: Unix Operating System Unsupported Version Detection*

Secondo il numero di versione riportato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.La mancanza di supporto implica che il fornitore non rilascerà alcuna nuova patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione: Esegui l'upgrade a una versione del sistema operativo Unix attualmente supportata.

3) *Critical: VNC Server "Password" Password*

Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "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.

4) **Critical:** ***Apache Tomcat AJP Connector Request Injection (Ghostcat)***

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice in modalità remota (RCE).
Soluzione: Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

5) **Critical:** ***SSL Version 2 and 3 Protocol Detection***

Secondo il numero di versione riportato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.
Soluzione: Esegui l'upgrade a una versione del sistema operativo Unix attualmente supportata.

6) **Critical:** ***Blind Shell Backdoor Detection***

Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "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.

7) **Critical:** ***SSL (Multiple Issues)***

La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.
Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.
Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle.
Soluzione: Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

8) *Critical: Samba Badlock Vulnerability*

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, che esiste nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici.

Soluzione: Aggiorna alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

9) *Critical: Nfs Shares World Readable*

Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP o intervallo IP).

Soluzione: Posizionare le opportune restrizioni su tutte le condivisioni NFS.