

NESSUS: VULNERABILITY ASSESSMENT METASPOITABLE

METASPOITABLE IP: 192.168.50.101

VULNERABILITIES TROVATE:

CRITICAL	HIGH	MEDIUM	LOW	INFO
9	5	24	5	122

SCAN INFORMATION:

Start Time: 24/11/2022 h.14:50

End Time: 24/11/2022 h.15:17

HOST INFORMATION:

Netbios Name: METASPOITABLE

IP: 192.168.50.101

MAC Address: 08:00:27:7B:21:1D

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

VULNERABILITIES HIGH

136769 - ISC BIND Service Downgrade / Reflected DoS

Description:

Un utente malintenzionato remoto non autenticato può sfruttarlo per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione.

Soluzione:

Aggiornamento alla versione ISC BIND a cui si fa riferimento nell'avviso del fornitore.

42256 - NFS Shares World Readable

Description:

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

Soluzione:

Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Description:

L'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di livello medio.

Si noti che è notevolmente più semplice aggirare la crittografia di media potenza se l'attaccante si trova sulla stessa rete fisica.

Soluzione:

Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrature di livello medio.