Scan Meta

Report generated by Nessus™ Thu, 24 Nov 2022 08:47:33 EST

Alaimo Alessandro
25/11/2022

Scansione Iniziale

192.168.50.101

51988 - Bind Shell Backdoor Detection

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.

Porta:

- tcp/1524/wild_shell

11356 - NFS Exported Share Information Disclosure

Descrizione:

- Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe essere in grado di sfruttare questa possibilità per leggere (ed eventualmente scrivere) i file sull'host remoto.

Soluzione:

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

Porta:

- udp/2049/rpc-nfs

61708 - VNC Server 'password' Password

Descrizione:

- Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un aggressore remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.

Soluzione:

- Proteggete il servizio VNC con una password forte.

Porta:

- tcp/5900/vnc

10203 - rexecd Service Detection

Descrizione:

- Il servizio rexecd è in esecuzione sull'host remoto. Questo servizio è stato progettato per consentire agli utenti di una rete di eseguire comandi in remoto. Tuttavia, rexecd non fornisce alcun buon mezzo di autenticazione, quindi può essere abusato da un utente malintenzionato per eseguire la scansione di un host di terze parti.

Soluzione:

- Commentare la riga 'exec' in /etc/inetd.conf e riavviare il processo inetd.

Porta:

- tcp/0