REPORT VULENRABILITA

PREMESSA

l CVSS (Common Vulnerability Scoring System) è un sistema standardizzato per valutare e assegnare un punteggio alle vulnerabilità dei sistemi informatici.

* Da 0 a 3.9: Vulnerabilità con un basso grado di rischio.
* Da 4.0 a 6.9: Vulnerabilità con un grado moderato di rischio.
* Da 7.0 a 8.9: Vulnerabilità con un grado elevato di rischio.
* Da 9.0 a 10.0: Vulnerabilità con un grado critico di rischio.

Le vulnerabilità di seguito riportate presentano un grado di vulnerabilità CVSS V3.0 di 9.8

1) Bind Shell Backdoor Detection

Questa vulnerabilità è associata a una possibile backdoor rilevata nel sistema. Una backdoor è una vulnerabilità o una porta d'accesso nascosta in un sistema informatico che consente a un attaccante di ottenere l'accesso non autorizzato e il controllo del sistema senza essere rilevato.

Azioni Consigliate:

1.Isolamento del Sistema: Isolare immediatamente il sistema vulnerabile dalla rete per impedire ulteriori accessi non autorizzati.

2. Analisi e Rimozione: Effettuare un'analisi approfondita del sistema per individuare e rimuovere la backdoor.

3. Verifica se l'host remoto è stato compromesso.

2) NFS Exported Share Information Disclosure

Spiegazione: Questa vulnerabilità è associata alla divulgazione non autorizzata di informazioni da parte di servizi NFS (Network File System). I servizi NFS condividono file e directory su una rete, e una configurazione errata può esporre informazioni sensibili a utenti non autorizzati.

Azioni Consigliate:

1.Potenziale per l'esecuzione di altri attacchi: Gli aggressori potrebbero utilizzare informazioni ottenute da una vulnerabilità di divulgazione per pianificare e lanciare ulteriori attacchi mirati. Ad esempio, potrebbero sfruttare le informazioni per ottenere accesso a sistemi con maggiori privilegi o per condurre attacchi di phishing mirati

2. Imposta le giuste autorizzazioni sui file e sulle directory condivise per garantire che solo gli utenti autorizzati possano accedervi.

3) UnrealIRCd Backdoor Detection

Spiegazione: Questa vulnerabilità è associata al rilevamento di una possibile backdoor nel software UnrealIRCd, che è un server Internet Relay Chat (IRC). IRC è un sistema di comunicazione in tempo reale basato su testo che consente a utenti di tutto il mondo di partecipare a conversazioni online attraverso canali dedicati.

Azioni Consigliate:

1.Isolamento del Sistema: Isolare immediatamente il sistema vulnerabile dalla rete per impedire ulteriori accessi non autorizzati.

2.Analisi e Rimozione: Effettuare un'analisi approfondita del sistema per individuare e rimuovere la backdoor.

3.Verifica se l'host remoto è stato compromesso.

4.disistalla e riinstalla e assicurati che siano presenti il checksum MD5 o SHA1(algoritmi di hash)

La verifica del checksum è un modo affidabile per accertarsi che il file scaricato sia identico alla versione originale fornita dalla fonte ufficiale.

4)VNC Server 'password' Password

Spiegazione: Questa vulnerabilità è associata al rilevamento di una password debole o predefinita associata a un server VNC (Virtual Network Computing). Le password deboli o predefinite possono consentire a un attaccante di accedere al sistema con facilità e potenzialmente ottenere il controllo dell'host.

Azioni Consigliate:

1.Cambio della Password: Cambiare immediatamente la password, assicurarsi che la nuova password sia complessa e non sia facilmente indovinabile.

2.Utilizzo di Autenticazione Due Fattori: Se possibile, utilizzare metodi di autenticazione a due fattori (2FA), per aumentare la sicurezza dell'accesso.

A screen shot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated