1. 61708 - VNC Server 'password' Password

Descrizione: Il server VNC remoto utilizza una password debole, in questo caso "password", consentendo a chiunque di accedere al server senza autenticazione.

Impatto e gravità:

Impatto: Critico, in quanto chiunque può accedere al server e prendere il controllo remoto del sistema.

CVSS: 10.0 (critico).

Soluzioni e mitigazioni:

Cambiare immediatamente la password VNC con una più forte.

Limitare l'accesso al server VNC tramite firewall e configurazioni di accesso sicuro.

Abilitare l’autenticazione a due fattori se supportata.

---

2. 42256 - NFS Shares World Readable

Descrizione: Il server NFS sta esportando condivisioni leggibili pubblicamente senza restrizioni di accesso, permettendo a chiunque di leggere i file condivisi.

Impatto e gravità:

Impatto: Medio, poiché i dati sensibili o critici possono essere esposti a chiunque nella rete.

CVSS v3.0 Base Score: 7.5 (alto).

Soluzioni e mitigazioni:

Limitare l'accesso alle condivisioni NFS tramite il file di configurazione /etc/exports, specificando gli host autorizzati.

Utilizzare Kerberos per autenticare l'accesso alle condivisioni NFS.

Assicurarsi che le condivisioni NFS siano accessibili solo da indirizzi IP affidabili.

---

3. 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Descrizione: Il server remoto supporta cifrari SSL a forza media, come 3DES, vulnerabili all'attacco SWEET32, che consente di decifrare il traffico crittografato.

Impatto e gravità:

Impatto: Medio, poiché un attaccante sulla stessa rete potrebbe decifrare il traffico crittografato.

CVSS v3.0 Base Score: 7.5 (alto).

Soluzioni e mitigazioni:

Disabilitare cifrari deboli come 3DES e utilizzare solo cifrari forti come AES.

Aggiornare la configurazione TLS per supportare solo TLSv1.2 o superiore.

Testare la configurazione SSL per assicurarsi che i cifrari deboli siano stati disabilitati.

---

4. 20007 - SSL Version 2 and 3 Protocol Detection

Descrizione: Il server accetta connessioni che utilizzano SSLv2 o SSLv3, protocolli obsoleti e vulnerabili a diversi attacchi crittografici, come POODLE.

Impatto e gravità:

Impatto: Critico, in quanto SSLv2 e SSLv3 sono considerati insicuri e vulnerabili a numerosi attacchi.

CVSS v3.0 Base Score: 7.5 (alto).

Soluzioni e mitigazioni:

Disabilitare SSLv2 e SSLv3 e utilizzare solo TLSv1.2 o superiore.

Verificare che il server non supporti più protocolli e cifrari deboli.

Testare la configurazione SSL con strumenti come SSL Labs Server Test.

---

5. 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

(SSL Check)

Descrizione: Il certificato SSL remoto è stato generato su un sistema Debian/Ubuntu affetto da una debolezza nel generatore di numeri casuali, rendendo la chiave SSL vulnerabile.

Impatto e gravità:

Impatto: Critico, poiché un attaccante potrebbe ottenere la chiave privata e decrittare le comunicazioni.

CVSS v2.0 Base Score: 5.0 (medio).

Soluzioni e mitigazioni:

Rigenerare tutti i certificati SSL e chiavi OpenSSH creati durante il periodo vulnerabile.

Aggiornare OpenSSL e assicurarsi di utilizzare una versione sicura.

Verificare l'uso di certificati SSL deboli con strumenti come ssh-vulnkey.

---

6. 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Descrizione: Il server SSH remoto utilizza chiavi generate su una versione vulnerabile di Debian/Ubuntu, con un generatore di numeri casuali compromesso, rendendo la chiave SSH vulnerabile.

Impatto e gravità:

Impatto: Critico, poiché un attaccante può ottenere la chiave privata e compromettere il server.

CVSS v2.0 Base Score: 5.0 (medio).

Soluzioni e mitigazioni:

Rigenerare tutte le chiavi SSH create durante il periodo di vulnerabilità.

Aggiornare OpenSSL e assicurarsi di utilizzare una versione sicura.

Utilizzare strumenti come ssh-vulnkey per identificare chiavi vulnerabili.