1. Apache Tomcat AJP Connector Request Injection (Ghostcat)(Critica)

Descrizione:
Una vulnerabilità nel connettore AJP consente a un attaccante non autenticato di leggere file sensibili o eseguire codice remoto (RCE) caricando file JSP.

Soluzione:

Aggiornare Apache Tomcat alle versioni **7.0.100**, **8.5.51**, **9.0.31** o superiori.

Configurare il connettore AJP per richiedere l'autenticazione e limitare l'accesso.

2. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness(Critica)

Descrizione:
Chiavi SSH e certificati SSL generati su questo sistema utilizzano un generatore di numeri casuali debole, permettendo a un attaccante di decifrare le connessioni o effettuare attacchi man-in-the-middle.

Soluzione:

Rigenerare tutte le chiavi SSH, SSL e OpenVPN utilizzando una versione aggiornata della libreria OpenSSL.

Aggiornare OpenSSL a una versione non affetta da questa vulnerabilità.

3. SSL Version 2 and 3 Protocol Detection(Critica)

Descrizione:
Il sistema supporta SSLv2 e SSLv3, protocolli obsoleti e vulnerabili ad attacchi come POODLE.

Soluzione:

Disabilitare SSLv2 e SSLv3 nella configurazione del server.

Abilitare TLS 1.2 o superiore con suite di cifratura approvate.

4. VNC Server Weak Password(Critica)

Descrizione:
Il server VNC è configurato con la password debole **"password"**, permettendo accesso non autorizzato al sistema.

Soluzione:

Configurare il server VNC con una password complessa e sicura.

Limitare l'accesso VNC tramite firewall.

5. Samba Badlock Vulnerability(Alta)

Descrizione:
La versione di Samba installata è vulnerabile a un attacco man-in-the-middle che può portare all'esecuzione di chiamate di rete arbitrarie nel contesto dell'utente intercettato.

Soluzione:

Aggiornare Samba alla versione **4.2.11**, **4.3.8**, **4.4.2** o superiore.

Implementare politiche di autenticazione più sicure per le connessioni SMB.