Alaimo Alessandro
24/11/2022

Report 3 Vulnerabilità Alte

34460 - Unsupported Web Server Detection

Descrizione:

- In base alla sua versione, il server Web remoto è obsoleto e non più gestito dal suo fornitore o provider. fornitore. La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza di conseguenza, potrebbe contenere vulnerabilità di sicurezza.

Soluzione:

- Rimuovere il server web se non è più necessario. Altrimenti, aggiornare a una versione supportata, se possibile, o passare a un altro server. passare a un altro server.

Rischio:

- Alto

Porta:

- tcp/8180/www

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.

Rischio:

- Alto

Porta:

- tcp/5900/vnc

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Descrizione:

- È stata riscontrata una vulnerabilità nella lettura/inclusione di file nel connettore AJP. Un aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione web da un server vulnerabile. Nei casi in cui il server server vulnerabile consente l'upload di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una serie di tipi di file, ottenendo così un

accesso remoto. una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione:

- Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo, 9.0.31 o successivo.

Rischio:

- Alto

Porta:

- tcp/8009/ajp13