REPORT TECNICO LORENZO SCORBAIOLI

ANALISI DI 3 CRITICITA’ DI LIVELLO HIGH

134862 - Apache Tomcat A JP Connector Request Injection (Ghostcat)

DESCRIZIONE

È stata rilevata una vulnerabilità di lettura/inclusione di file in un connettore JP. Potrebbe farlo un utente malintenzionato remoto e non autenticato sfruttare questa vulnerabilità per leggere i file dell'applicazione Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

SOLUZIONE

Aggiorna la configurazione A JP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

PLUGIN OUTPUT

tcp/8009/ajp13

RISK FACTOR

High

Non essendoci nel report altri rischi di livello high ne ho presi 2 di livelli critico.

51988 - Bind Shell Backdoor Detection

DESCRIZIONE

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può usarlo da collegandosi alla porta remota e inviando direttamente i comandi.

SOLUZIONE

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

PLUGIN OUTPUT

tcp/1524/wild_shell

RISK FACTOR

Critical

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

DESCRIZIONE

La chiave dell'host SSH remoto è stata generata su un sistema Debian o Ubuntu che contiene un bug nel file generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto a un packager Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per impostare la decifrazione del telecomando sessione o impostare un uomo nel mezzo dell'attacco.

SOLUZIONE

Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutti gli SSH, Il materiale delle chiavi SSL e OpenVPN deve essere rigenerato.

PLUGIN OUTPUT

tcp/22/ssh

RISK FACTOR

Critical