VULNERABILITA' ALTE

134862 – Apache Tomcat AJP Connector Request Injection (Ghostcat)

DESCRIZIONE

È stata rilevata una vulnerabilità di lettura/inclusione di file in un connettore JP. Un utente malintenzionato remoto e non autenticato potrebbe 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 di 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.

FATTORE DI RISCHIO: ALTO

Plugin Output
tcp/8009/ajp13

136769 - ISC BIND Service Downgrade / Reflected DoS

DESCRIZIONE

Secondo la sua versione auto-segnalata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è interessata dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Ciò è dovuto al fatto che BIND DNS non limita sufficientemente il numero di recuperi che possono essere eseguiti durante l'elaborazione di una risposta di riferimento.
Un utente malintenzionato remoto non autenticato può sfruttarlo per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione.

SOLUZIONE

Aggiornamento alla versione ISC BIND a cui si fa riferimento nell'avviso del fornitore.

FATTORE DI RISCHIO: ALTO

Plugin Output
udp/53/Ddns

42256 - NFS Shares World Readable

DESCRIZIONE

Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (basato su nome host, IP o intervallo IP).

SOLUZIONE

Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

FATTORE DI RISCHIO: ALTO

Plugin Output
Tcp/2049/rpc-nfs