Floriana Feminò

24/11/2022

VULNERABILITY ASSESSMENT – REPORT TECNICO

Informazioni sulla scansione

Inizio: 24/11/ 2022 14:53:49

Termine: 24/11/2022 15:23:25

Informazioni sull'host

Netbios Name: METASPLOITABLE

IP: 192.168.90.101

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

VULNERABILITA'

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

Descrizione:

È stata riscontrata una vulnerabilità di lettura/inclusione di file in A JP Connector. 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 vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una serie di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione:

Aggiornare la configurazione di 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 - Downgrade del Servizio ISC BIND / DoS riflesso

Descrizione:

Secondo la versione auto-riportata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è affetta da vulnerabilità di downgrade delle prestazioni e DoS riflesso. Ciò è dovuto al fatto che BIND DNS non limita sufficientemente il numero di fetch che possono essere eseguiti durante l'elaborazione di una risposta di riferimento. Un aggressore remoto non autenticato può sfruttare questa situazione per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione.

Soluzione:

Aggiornare alla versione di ISC BIND indicata nell'avviso del fornitore.

Fattore di rischio: Medio

Plugin Output: udp/53/dns

42256 - Condivisioni NFS leggibili da tutti

Descrizione:

Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a hostname, IP o intervallo di IP).

Soluzione:

Applicare le appropriate restrizioni su tutte le condivisioni NFS.

Fattore di rischio: Medio

Plugin Output: tcp/2049/rpc-nfs