CUORE ANDREA

24-11-2022

REPORT VULNERABILITA' METASPLOITABLE – FATTORE DI RISCHIO 7

Host: 192.168.50.101

Netbios Name: METASPLOITABLE

OS: Linux Kernel 2.6 on Ubuntu 8.04

- 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
  - Porta: TCP/25/smtp
  - Descrizione: L'host remoto supporta l'uso di cifrari SSL che offrono una crittografia di media forza. Per media forza si intende qualsiasi crittografia che utilizzi chiavi di lunghezza pari ad almeno 64 bit e inferiore a 112bit, oppure che utilizza la suite di crittografia 3DES. Si noti che è molto più facile aggirare la crittografia a media resistenza se l'aggressore si trova sulla stessa rete fisica.
  - Fattore di rischio: HIGH-MEDIUM (7.5)
  - Soluzione: Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di cifrari a media forza.

- 136769 - ISC BIND Service Downgrade / Reflected DoS
  - Porta: UDP/53/dns
  - 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 risponsta di rinvio. Un aggressore da remoto non autenticato può sfruttare questa situazione per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come un server riflesso.
  - Fattore di rischio: MEDIUM-HIGH (7.5)
  - Soluzione: Aggiornare alla versione di ISC BIND indicata dal fornitore.

- 134862 - Apache Tomcat A JP Connector Request Injection (Ghostcat)
  - Porta: TCP/8009/ajp13
  - Descrizione: È stata riscontrata una vulnerabilità di lettura/inclusione di file in A JP connector. Un aggressore 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 l'upload di file, un utente malintenzionato potrebbe caricare il codice JavaServer Pages (JSP) dannoso all'interno di una seria di tipi di file, ottenendo cosi un accesso remoto. Una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

- Fattore di rischio: HIGH
- Soluzione: Aggiornare la configurazione di AJP per richiedere l'autorizzazione e/o aggiornare il server tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo