Esercizio Epicode 26.10.2023

Spiegazione delle prime 4 Vulnerabilità su Metaspoitable

1) Apache Tomcat AJP Connector Request Injection (Ghostcat)

La vulnerabilità consente a un attaccante, in remoto non autenticato, di accedere caricando codici malevoli JSP (JavaServer Pages) per poi visualizzare file sensibili all'interno del sistema ospite del server Tomcat, come file di configurazione o risorse web protette.

Per mitigare questa vulnerabilità, è consigliabile aggiornare il Server Tomcat al 7.0.100, 8.5.51, 9.0.31 o versioni successive. Queste versioni includono la patch di sicurezza per CVE-2020-1938 che aumenta la sicurezza del server rafforzando le autenticazioni da parte delle richieste AJP e limitando l'accesso ai file più sensibili all'interno di Tomcat.

2) Bind Shell Backdoor Detection

Nessus ha rilevato una shell in ascolto sulla porta 1524 (wild_shell) senza che sia richiesta alcuna autenticazione. Un attaccante può usare questa porta come backdoor.

In questo caso è necessario controllare se l'host ha compromesso la macchina e reinstallare da capo il sistema operativo.

3) SSL Version 2 and 3 Protocol Detection

I protocolli SSL (V2 e V3) rilevati nella macchina Metaspoitable hanno versioni obsolete con diversi punti deboli nel crittografare i pacchetti. Un attaccante MITM potrebbe eseguire un exploit, per esempio tramite un attacco POODLE, sui dati crittografati e decriptarli.

Per mitigare questa vulnerabilità, è consigliabile disabilitare i protocolli ssl v2, v3 ed utilizzare protocolli TLS v1.2 o versioni successive.

N.B. Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure.

4) Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution

È stata rilevata una vulnerabilità di esecuzione del codice in remoto con una versione Apache Log4J precedente alla 2.16.0, a causa di protezioni insufficienti durante le sostituzioni dei messaggi di ricerca dati in input dall'utente. Un attaccante in remoto, non autenticato, può effettuare un exploit tramite una richiesta Web per eseguire il codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Per mitigare questa vulnerabilità, è consigliabile aggiornare Apache Log4j alla versione 2.0.16 o successive