Report Nessus

Esplorazione del software Nessus:

Settato il lab in ambiente virtuale con Kali,Metasploitable,WindowsXp

Ho generato inizialmente 2 report sulla macchina metasploitable in modo rapito per capire il funzionamento, ho provato anche sulla macchina xp e infine ho riprovato sulla macchina metasploitable generando un report più completo e uno esteso aggiungendo

(in allegato i report).

Ho cercato di prendere confidenza col software nonostante le difficoltà del mio dispositivo

Approfondimento sulle Vulnerabilità di Metasploitable :

Apache Tomcat AJP Connector Request Injection (Ghostcat):

Porte specifiche: (8009 per AJP).

Versioni affette: Dettaglio delle versioni vulnerabili.

CVE associata: CVE-2020-1938 (Ghostcat)

Quando si utilizza il protocollo Apache JServ Protocol (AJP), è necessario prestare attenzione nell'affidarsi alle connessioni in entrata verso Apache Tomcat. Tomcat tratta le connessioni AJP con un livello di fiducia più elevato rispetto, ad esempio, a una connessione HTTP simile. Se tali connessioni sono accessibili a un attaccante, possono essere sfruttate in modi inaspettati.

Prima della versione 7.0.100, Tomcat veniva fornito con un connettore AJP abilitato per impostazione predefinita, che ascoltava su tutti gli indirizzi IP configurati. Era previsto (e raccomandato nella guida alla sicurezza) che questo connettore venisse disabilitato se non necessario.

Rischi Conosciuti Prima della Segnalazione:

Aggiramento dei controlli di sicurezza basati sull'indirizzo IP del client: Gli attaccanti potevano ignorare le restrizioni IP.

Aggiramento dell'autenticazione: Se Tomcat era configurato per fidarsi dei dati di autenticazione forniti dal reverse proxy, gli attaccanti potevano sfruttare questa configurazione.

Vulnerabilità Identificata:

Accesso a file arbitrari: Era possibile restituire file da qualsiasi punto dell'applicazione web, comprese directory sensibili come WEB-INF e META-INF, o qualsiasi altra directory accessibile tramite ServletContext.getResourceAsStream().

Elaborazione di file come JSP: Qualsiasi file presente nell'applicazione poteva essere elaborato come JSP, eseguendo potenzialmente codice dannoso.

Se l'applicazione web consentiva il caricamento di file e li memorizzava all'interno della stessa applicazione (o se l'attaccante riusciva a controllare il contenuto dell'applicazione in altro modo), questa vulnerabilità, combinata con l'esecuzione di file JSP, rendeva possibile l'esecuzione remota di codice (RCE).

Mitigazione:

È importante notare che la mitigazione è necessaria solo se una porta AJP è accessibile a utenti non attendibili. Gli utenti che desiderano adottare un approccio di difesa più approfondito e bloccare il vettore che consente l'accesso a file arbitrari e l'esecuzione di JSP possono aggiornare a Apache Tomcat 9.0.31 o versioni successive.

Si noti inoltre che sono state apportate diverse modifiche alla configurazione predefinita del connettore AJP nella versione 7.0.100 per migliorarne la sicurezza. Gli utenti che effettuano l'aggiornamento a questa versione o successive potrebbero dover apportare piccole modifiche alle loro configurazioni esistenti.

Bind Shell Backdoor Detection:

Descrizione: Accesso remoto tramite una porta aperta controllata dall'attaccante, utilizzata per eseguire comandi sul sistema compromesso.

Porta: Variabile (spesso porte elevate >1024).

Mitigazione: Monitorare porte aperte, aggiornare firewall e abilitare sistemi di rilevamento delle intrusioni (IDS).

Debian OpenSSH/OpenSSL RNG Weakness:

Descrizione: Chiavi crittografiche prevedibili generate su sistemi Debian vulnerabili, compromettendo la sicurezza SSH.

Porta: 22 (SSH).

Mitigazione: Aggiornare OpenSSL/OpenSSH e rigenerare tutte le chiavi SSH.

Debian OpenSSH/OpenSSL RNG Weakness (SSL Check):

Descrizione: Certificati SSL generati con numeri casuali deboli, vulnerabili ad attacchi MITM.

Porta: 443 (HTTPS) e altre porte SSL/TLS.

Mitigazione: Aggiornare OpenSSL e sostituire tutti i certificati SSL compromessi.

References

identificatori standard utilizzati nei report di sicurezza per riferirsi a vulnerabilità conosciute, exploit e advisory.

BID (Bugtraq ID):

Un identificatore unico assegnato a una vulnerabilità nel database di Bugtraq, un archivio storico di vulnerabilità.

Utilizzato da diverse piattaforme di sicurezza per riferirsi a vulnerabilità documentate.

Esempio: BID-12345

CVE (Common Vulnerabilities and Exposures):

Uno standard globale per identificare vulnerabilità di sicurezza.

Ogni CVE è assegnato dal Mitre Corporation e seguito da un anno e un numero univoco.

Utilizzato nei database di sicurezza come NVD (National Vulnerability Database).

Esempio: CVE-2023-4567

XREF (Cross-Reference):

Indica riferimenti incrociati ad altre fonti che descrivono la stessa vulnerabilità, come advisories di fornitori, bollettini di sicurezza o articoli tecnici.

Consente di ottenere una visione più completa di una vulnerabilità consultando diverse fonti.

Esempio: XREF-MSFT-2023-001 (riferimento incrociato a un advisory Microsoft).

Conclusioni:

Il software Nessus risulta molto interessante e utile per effettuare dei report dettagliati, purtroppo a causa delle mie limitazioni Hardware per il momento non ho potuto approfondire oltre.

BID (Bugtraq ID):

Identificatore unico per vulnerabilità registrate nel database Bugtraq.

Esempio: BID-12345

CVE (Common Vulnerabilities and Exposures):

Standard globale per identificare vulnerabilità di sicurezza.

Assegnato da Mitre con un anno e un numero univoco.

Esempio: CVE-2023-4567

XREF (Cross-Reference):

Riferimento incrociato ad altre fonti che descrivono la stessa vulnerabilità, come advisories o bollettini di sicurezza.

Esempio: XREF-MSFT-2023-001