GHOSTCAT

Ghostcat sfrutta configurazioni non sicure dell'AJP Connector di Apache Tomcat per consentire accessi non autorizzati ai file e potenzialmente eseguire codice malevolo.

Cos'è l'AJP?
L'AJP Connector è un componente utilizzato nei server web e nei server di applicazioni per gestire le comunicazioni tramite il protocollo AJP (Apache JServ Protocol) Il suo ruolo principale è quello di facilitare il trasferimento efficiente delle richieste HTTP dal web server all'application server e delle risposte HTTP dall'application server al web server. Questo avviene grazie al fatto trasmette i dati in codice binario così da rendere più snella la comunicazione.

Descrizione di un attacco Ghostcat

- L'attaccante inizia con una scansione di rete per identificare server che eseguono Apache Tomcat. Tramite strumenti come Nmap può trovare la porta aperte dell'AJP Connector (di default la porta è la 8009)
- Dopo aver individuato un server con la porta 8009 aperta, l'attaccante verifica se l'AJP Connector è vulnerabile tramite strumenti come ajpShooter o script personalizzati che possono essere utilizzati per inviare richieste AJP.
- Se il server è vulnerabile, l'attaccante invia richieste AJP per leggere file sensibili sul server.

NFS Exported Share Information Disclosure

NFS è un protocollo di rete standard che consente a sistemi operativi UNIX-like di montare condivisioni di file da un server NFS remoto. L'exploit in questione sfrutta il fatto che le condivisioni NFS esportate da un server possono rivelare informazioni sensibili, come percorsi di file, configurazioni di rete, e altre informazioni di sistema.

Descrizione di un attacco su NFS

Gli attaccanti interrogano un server NFS per ottenere una lista dei file delle condivisioni di file esportate. Questo può essere fatto utilizzando strumenti come `showmount` (che è un commando per visualizzare la condivisione dei file) in ambiente UNIX o attraverso richieste RPC (Remote Procedure Call) manipolate. Ottenendo informazioni su condivisioni esportate, gli attaccanti possono mappare la struttura di file directory del server NFS, identificare file sensibili, scoprire configurazioni di rete e trovare punti deboli nel sistema. Gli attaccanti possono utilizzare queste informazioni per pianificare ulteriori attacchi, come tentativi di accesso non autorizzato a file sensibili, eseguire attacchi di tipo directory traversal o preparare attacchi mirati basati sulla conoscenza della topologia di rete e delle configurazioni di sistema.

SSL Version 2 and 3 Protocol Detection

SSL (Secure Sockets Layer) Version 2 e Version 3 sono protocolli crittografici obsoleti utilizzati per la comunicazione sicura su una rete informatica. Tuttavia, presentavano diverse vulnerabilità di sicurezza.

SSLv2 e il SSLv 3 sono noti per avere diverse vulnerabilità e debolezze che le rendono insicure e inadeguate per proteggere le comunicazioni su reti non sicure. Alcune delle vulnerabilità più importanti sono:
Crittografia Debole: supportano algoritmi di crittografia deboli, come DES a 40 bit e RC2 a 40 bit, che possono essere facilmente craccati con tecniche di forza bruta.
Nessuna Protezione per l'Integrità della Connessione: non forniscono un'adeguata protezione per l'integrità della connessione. Non includono un meccanismo per garantire che i dati non siano stati alterati durante il transito.
Attacchi di Intercettazione (Man-in-the-Middle): La mancanza di protezione dell'integrità e la debolezza degli algoritmi di crittografia rendono SSLv2 e SSLv3 vulnerabili agli attacchi Man-in-the-Middle (MitM), dove un attaccante può intercettare e modificare i dati scambiati tra il client e il server.
Nessuna Protezione Contro gli Attacchi di Downgrade: Non hanno meccanismi efficaci per prevenire gli attacchi di downgrade, dove un attaccante forza il client e il server a utilizzare una versione inferiore e meno sicura del protocollo.
Attacchi di Riutilizzo delle Chiavi: Non generano chiavi di sessione uniche per ogni connessione, il che significa che le stesse chiavi possono essere riutilizzate. Questo rende più facile per un attaccante craccare la crittografia e decifrare le comunicazioni.
Scarsa Protezione dei Certificati: hanno meccanismi inadeguati per la gestione e la validazione dei certificati digitali, rendendo più facile per gli attaccanti presentare certificati falsi o manomessi.
Supporto Limitato per Algoritmi di Hash: utilizzano algoritmi di hash deboli, come MD5, che sono suscettibili agli attacchi di collisione. Questo significa che gli attaccanti possono creare messaggi diversi con lo stesso valore di hash, compromettendo l'integrità dei dati.

Le debolezze di SSLv2 e SSLv3 hanno gravi implicazioni per la sicurezza delle comunicazioni:

- **Furto di Dati**: Le comunicazioni crittografate con SSLv2 possono essere facilmente decrittografate, esponendo dati sensibili come informazioni personali, credenziali di accesso e dettagli finanziari.
- **Manipolazione dei Dati**: Gli attaccanti possono intercettare e modificare i dati trasmessi, compromettendo l'integrità delle informazioni.