Analisi vulnerabilità del sistema informatico metasploitable2

Introduzione

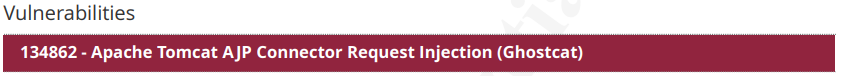
In seguito ad una scansione di Nessus, è stato rilevato che Metasploitable2 presenta numerose vulnerabilità e falle di sicurezza, che rendono il sistema altamente vulnerabile ad attacchi esterni. Queste vulnerabilità rappresentano una potenziale minaccia per la sicurezza delle informazioni e dei dati presenti sulla macchina virtuale. Pertanto, questo report fornisce un'analisi dettagliata delle principali vulnerabilità riscontrate in Metasploitable2 e descrive come queste possono essere sfruttate per compromettere la sicurezza del sistema.

Metodologia

Per l'analisi delle vulnerabilità è stata utilizzata la versione di Nessus 8.8.0. Il profilo di scansione creato è stato configurato per eseguire una scansione completa delle vulnerabilità su tutti i sistemi disponibili in Metasploitable. Le opzioni di scansione includono la scansione delle porte, l'individuazione del sistema operativo e la scansione delle vulnerabilità, con il livello di rischio impostato su "Critical".



In questo report elencheremo unicamente le vulnerabilità critiche



Descrizione

È stata riscontrata una vulnerabilità nella lettura/inclusione di file in AJP 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

server vulnerabile consente l'upload di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una serie di tipi di file e ottenere un accesso remoto.

una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione

Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo,

9.0.31 o successivo.



Descrizione

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla

connettendosi alla porta remota e inviando direttamente i comandi.

Soluzione

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.



Descrizione

La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della libreria OpenSSL.

generatore di numeri casuali della libreria OpenSSL.

Il problema è dovuto alla rimozione da parte di un packager Debian di quasi tutte le fonti di entropia nella versione remota di

OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e usarla per decifrare la sessione remota o per creare una sessione

sessione remota o impostare un attacco man in the middle.

Soluzione

Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale delle chiavi SSH,



Descrizione

Il certificato x509 sul server SSL remoto è stato generato su un sistema Debian o Ubuntu

che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto alla rimozione da parte di un packager Debian di quasi tutte le fonti di entropia nella versione remota di

OpenSSL.

Un aggressore può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota

o impostare un attacco man in the middle

Soluzione

Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale delle chiavi SSH,

SSL e OpenVPN devono essere rigenerati.



Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un

attaccante potrebbe essere in grado di sfruttare questa possibilità per leggere (ed eventualmente scrivere) i file sull'host remoto.

Soluzione

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.



Descrizione del servizio

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono

sono affette da diversi difetti crittografici, tra cui:

- Uno schema di imbottitura insicuro con i cifrari CBC.

- Schemi di rinegoziazione e ripresa della sessione non sicuri.

Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o per decriptare le comunicazioni tra il servizio interessato e i client.

tra il servizio interessato e i client.

Sebbene SSL/TLS disponga di un metodo sicuro per scegliere la versione più alta del protocollo supportata (in modo che queste versioni vengano utilizzate solo se

che queste versioni vengano utilizzate solo se il client o il server non supportano nulla di meglio), molti browser web lo implementano in modo

implementano questo metodo in modo non sicuro, consentendo a un aggressore di declassare una connessione (come nel caso di POODLE).

Pertanto, si raccomanda di disabilitare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di

di applicazione prevista da PCI DSS v3.1, qualsiasi versione di SSL non soddisfa la definizione di "crittografia forte" data da PCI SSC.

crittografia forte".

Soluzione

Consultate la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0.

Utilizzare invece TLS 1.2 (con suite di cifratura approvate) o superiore.



Descrizione

Secondo il numero di versione dichiarato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.

non è più supportato.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza

di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione

Aggiornare a una versione del sistema operativo Unix attualmente supportata.

Descrizione

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad accedere

utilizzando l'autenticazione VNC e una password "password". Un aggressore remoto e non autenticato potrebbe sfruttare questo

questo per prendere il controllo del sistema.

Soluzione

Proteggere il servizio VNC con una password forte

Conclusioni

Conclusioni:L'analisi delle vulnerabilità di Metasploitable utilizzando Nessus ha evidenziato un numero significativo di vulnerabilità che potrebbero rappresentare una minaccia per la sicurezza delle informazioni e dei dati aziendali. Per mitigare questi rischi, si consiglia di adottare le seguenti azioni correttive:• Aggiornare regolarmente i sistemi operativi e i software applicativi utilizzati in Metasploitable, al fine di prevenire eventuali vulnerabilità note;• Installare su una macchina pfsense, dandogli delle regole di filtraggio, per poter prevenire eventuali attacchi informatici.