Esercizio 04/12/2024

Esercizio 04/12/2024

Scan Information

Start time: Wed Dec 4 08:11:22 2024
End time: Wed Dec 4 08:32:19 2024

Host Information

```
Netbios Name: METASPLOITABLE
IP: 192.168.10.10
MAC Address: 08:00:27:4D:E1:90
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
```

Vulnerabilities

- Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

ID Plugin: 32321

Sinossi

Il certificato SSL remoto utilizza una chiave debole.

Descrizione

Il certificato x509 è stato generato su un sistema Debian o Ubuntu con un bug nell'OpenSSL, dovuto alla rimozione di fonti di entropia. Un attaccante può ottenere la chiave privata e decifrare la sessione o eseguire un attacco man-in-the-middle.

Informazioni aggiuntive

CVE-2008-0166

```
Pacchetto: openssl
Vulnerabilità: Generatore di numeri casuali prevedibile (CVE-2008-0166)
Tipo di problema: remoto, specifico per Debian
```

Il generatore di numeri casuali di OpenSSL su Debian è prevedibile a causa di una modifica errata, che rende le chiavi crittografiche facilmente indovinabili. Questo problema riguarda solo Debian, ma può

influenzare altri sistemi se importano chiavi vulnerabili.

Impatto

Le chiavi SSH, OpenVPN, DNSSEC, X.509 e SSL/TLS sono vulnerabili.
Le chiavi DSA su Debian compromesse sono particolarmente a rischio.

Soluzione

Considera tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutte le chiavi SSH, SSL e OpenVPN dovrebbero essere rigenerate.

Rischio

Critico.

Plugin Information

Published: 2008/05/14, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

SSL Version 2 and 3 Protocol Detection

ID Plugin: 32321

Sinossi

Il servizio remoto cifra il traffico usando un protocollo con vulnerabilità note.

Descrizione

Il servizio accetta connessioni cifrate con SSL 2.0 e/o SSL 3.0, vulnerabili a difetti crittografici come un padding insicuro e problemi di rinegoziazione delle sessioni. Un attaccante può sfruttarli per attacchi man-in-the-middle o decrittare le comunicazioni. Si consiglia di disabilitare completamente questi protocolli, poiché SSL 3.0 non è più considerato sicuro.

Informazioni aggiuntive

SSLv2 è vulnerabile a diversi difetti crittografici ed è stato deprecato. Un attaccante potrebbe sfruttare queste debolezze per attacchi man-in-the-middle o per decriptare le comunicazioni. Per disabilitare SSLv2 in Apache, segui questi passaggi:

1. Modifica il file /etc/httpd/conf.d/ssl.conf
2. Verifica la disabilitazione di SSLv2 eseguendo
3. Assicurarsi che il server funzioni correttamente con SSLv3 o TLSv1.

Soluzione

Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Usa invece TLS 1.2 (con suite di cifratura approvate) o versioni superiori.

Rischio

Critico

Plugin Output

tcp/25/smtp

SSL Medium Strength Cipher Suites Supported (SWEET32)

ID Plugin: 42873

Sinossi

Il servizio remoto supporta l'uso di cifrari SSL a forza media.

Descrizione

Il servizio remoto supporta cifrari SSL che offrono una crittografia a forza media, definita come crittografia con lunghezze di chiave tra 64 e 112 bit, o l'uso della suite di cifratura 3DES. La crittografia a forza media è vulnerabile a elusioni, specialmente se l'attaccante si trova sulla stessa rete fisica.

Soluzione

Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrari a forza media.

Rischio

Critico

Plugin Information

Published: 2017/06/22, Modified: 2022/04/11

Plugin Output

tcp/80/www