MACCHINA TARGET: Metasploitable

INDIRIZZO IP: 192.168.50.101

MAC ADDRESS: 08:00:27:88:44:EC

SISTEMA OPERATIVO: Unix

dalla scansione sono risultate 25 vulnerabilità critiche, 92 ad alto rischio, 131 con rischio medio e 16 a basso

32314 - Debolezza nel Generatore di Numeri Casuali nei Pacchetti Debian OpenSSH/OpenSSL

Sinossi:
Le chiavi host SSH remote sono deboli.

Descrizione:
La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu con un bug nel generatore di numeri casuali della libreria OpenSSL.
Il problema è stato causato da un pacchettizzatore Debian che ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.
Un attaccante può ottenere facilmente la parte privata della chiave remota, usandola per decifrare la sessione remota o per impostare un attacco di tipo "man in the middle".

CVSS Base Score 10.0:

Questo punteggio indica un rischio massimo, dove l'attaccante può sfruttare la vulnerabilità senza necessità di autenticazione, con un impatto completo su confidenzialità, integrità e disponibilità.

CVE-2008-0166:

Descrive il difetto nel generatore di numeri casuali che causa debolezza nella creazione di chiavi crittografiche. La vulnerabilità è stata introdotta nella versione di OpenSSL patchate da debian tra il 2006 e il 2008, documentandomi sul sito exploit db ho notato che questa vulnerabilità di openSSL su debian fa si che ci siano solo 65.538 possibili chiavi SSH generate, poichè l' unica entropia disponibile è il PID del processo che genera la chiave e questo potrebbe essere un vettore di attacco utilizzando un attacco di tipo brute force.

Dai link riportati nel report della scansione di nessun :
https://lists.debian.org/debian-security-announce/2008/msg00152.html

https://lists.ubuntu.com/archives/ubuntu-security-announce/2008-May/000705.html

Ho potuto leggere che questa vulnerabilità poteva essere sfruttata solo su macchine basate su un' architettura Debian e Ubuntu.

Per quanto riguarda la vulnerabilità su Debuab è stato risolto un bug critico che rende prevedibile il generatore di numeri casuali usato per creare chiavi crittografiche. Il problema ha coinvolto chiavi SSH, OpenVPN, DNSSEC e certificate SSL/TLS, richiedendo la rigenerazione di tutte le chiavi generate con OpenSSL sui sistemi vulnerabili.

mentre l'altro link riportava dettagli sulla necessità di rigenerare le chiavi e sulla distribuzione di pacchetti aggiornati per mitigarne gli effetti.

Vulnerabilità 20007 - SSL Version 2 and 3 Protocol Detection

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

Descrizione:
Il servizio remoto accetta connessioni crittografate con SSL 2.0 e/o SSL 3.0. Queste versioni di SSL presentano molteplici vulnerabilità crittografiche, tra cui:

- Schema di padding insicuro con cifrari CBC.
- Schemi insicuri di negoziazione e ripresa delle sessioni.

Un attaccante può sfruttare queste vulnerabilità per eseguire attacchi man-in-the-middle o decifrare comunicazioni tra il servizio e i client.
Sebbene SSL/TLS includa un metodo sicuro per selezionare la versione più alta del protocollo supportata, molte implementazioni dei browser consentono il downgrade a una versione meno sicura (es. attacco POODLE).

Il NIST ha determinato che SSL 3.0 non è più accettabile per comunicazioni sicure, e il PCI DSS v3.1 stabilisce che nessuna versione di SSL soddisfa i criteri di "crittografia forte".

Riferimenti utili:

- Paper di Schneier su SSL
- Attacco POODLE descritto da OpenSSL
- RFC7507 - POODLE
- RFC7568 - Disabilitazione di SSL 3.0

Soluzione:
Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Usare TLS 1.2 (o superiore) con cifrari approvati.

Fattore di rischio:
Critico.

Punteggi di rischio:

- **CVSS v3.0 Base Score:** 9.8 *(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)*
- **CVSS v2.0 Base Score:** 10.0 *(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)*

ANALISI DELLA VULNERABILITÀ:

Crittografia debole (SSLv2 e SSLv3):

Le versioni di SSL specificate supportano cifrari con chiavi inferiori a 64 bit, rendendoli suscettibili ad attacchi di forza bruta.

Schemi come CBC (Cipher Block Chaining) soffrono di problemi di padding, sfruttabili per estrarre informazioni dai messaggi cifrati.

Classificazione delle vulnerabilità dei cifrari:

Cifrari di bassa forza (<= 64-bit):

Vulnerabili agli attacchi di forza bruta e facilmente decifrabili. Esempi: EXP-RC2-CBC-MD5, EXP-RC4-MD5.

Cifrari di media forza (> 64-bit e < 112-bit):

Esempio: DES-CBC3-MD5 (3DES), considerato meno sicuro rispetto agli standard moderni.

Cifrari di alta forza (>= 112-bit):

RC4-MD5, nonostante l'elevata lunghezza della chiave, è considerato insicuro a causa di debolezze nel flusso di cifratura RC4.

Attacchi di downgrade e POODLE:

Gli attaccanti possono forzare il protocollo a usare versioni deboli di SSL tramite attacchi di downgrade, come evidenziato nell'attacco POODLE (Padding Oracle On Downgraded Legacy Encryption).

Vulnerabilità 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

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

Descrizione:
L'host remoto consente l'uso di cifrari SSL che forniscono crittografia di media forza.
Secondo Nessus, si considerano cifrari di media forza quelli con chiavi lunghe almeno 64 bit ma inferiori a 112 bit, oppure quelli che utilizzano la suite di cifratura 3DES.
Questi cifrari sono più vulnerabili, specialmente se un attaccante si trova sulla stessa rete fisica dell'host.

Riferimenti utili:

- Post di OpenSSL su SWEET32
- Sito SWEET32

Soluzione:
Riconfigurare l'applicazione interessata per evitare l'uso di cifrari di media forza.

Fattore di rischio:
Medio.

Punteggi di rischio:

- **CVSS v3.0 Base Score:** 7.5 *(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)*
- **CVSS v2.0 Base Score:** 5.0 *(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)*

CVE correlati:

- CVE-2016-2183

Analisi dettagliata:

1. **Cifrari di media forza e vulnerabilità SWEET32:**
    - I cifrari a media forza come 3DES (utilizzato nel Cipher Block Chaining) sono suscettibili a attacchi basati sulla collezione di grandi volumi di dati (attacco SWEET32).
    - Questo tipo di attacco sfrutta la possibilità di collisioni nel cifrario quando si cifrano grandi quantità di dati.
2. **Rischi principali:**
    - **Crittografia debole:** Cifrari con chiavi tra 64 e 112 bit sono più facili da decifrare con attacchi moderni.
    - **Vulnerabilità specifica di 3DES:** Il cifrario 3DES è noto per essere lento e vulnerabile rispetto agli standard moderni.
3. **Cifrari identificati nel report:**
    - **DES-CBC3-MD5:** Utilizza 3DES con MAC MD5.
    - **EDH-RSA-DES-CBC3-SHA:** Utilizza 3DES con autenticazione RSA e SHA1.

    - **ADH-DES-CBC3-SHA:** Autenticazione anonima (DH), quindi altamente vulnerabile.
4. Questi cifrari sono considerati di media forza perché utilizzano 3DES, che ha una lunghezza effettiva della chiave di 112 bit.
5. **Azioni raccomandate:**
    - Disabilitare i cifrari 3DES e qualsiasi altro cifrario di media forza.
    - Implementare solo cifrari moderni e sicuri, come AES con lunghezza di chiave di almeno 128 bit.
    - Aggiornare le librerie OpenSSL o simili per supportare configurazioni sicure.
6. **Impatto di un attacco SWEET32:**
    - Un attaccante sulla stessa rete può sfruttare i cifrari deboli per decifrare una sessione intercettando una quantità significativa di dati.