CRITICITA' RILEVATE IN NESSUNS

Analisi delle criticità, come difendersi e come mitigarle

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

CRITICAL	10.0*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness

Descrizione vulnerabilità:

Il problema di sicurezza CVE-2008-0166 riguarda una debolezza nel generatore di numeri casuali del pacchetto OpenSSL su Debian e sistemi derivati, che è stato introdotto a causa di un errore nella modifica del pacchetto OpenSSL da parte di Debian. Questo errore ha ridotto significativamente la qualità della randomicità utilizzata per la generazione di chiavi crittografiche, rendendo le chiavi SSH e altri materiali crittografici facilmente prevedibili. In pratica, venivano generate solo 65.536 chiavi SSH possibili, poiché l'unica randomicità utilizzata era il PID del processo generatore. Le chiavi compromesse includono quelle SSH, OpenVPN, DNSSEC, X.509 e quelle usate per le sessioni SSL/TLS. Le chiavi generate con GnuPG o GNUTLS non sono invece interessate.

Possibili rischi di attacchi:

La vulnerabilità nel generatore di numeri casuali del pacchetto OpenSSL su Debian (CVE-2008-0166) potrebbe portare a vari tipi di attacchi. Alcuni dei principali attacchi che potrebbero interessare questa vulnerabilità includono:

1. **Attacco Man-in-the-Middle (MITM):** Poiché le chiavi SSH e SSL generate con il generatore di numeri casuali compromesso sono prevedibili, un attaccante che intercetta la comunicazione potrebbe usare una chiave vulnerabile per decifrare o manipolare la comunicazione o permettendo l'accesso non autorizzato.
2. **Brute Force delle Chiavi SSH**: Poiché la debolezza nel generatore di numeri casuali riduce significativamente lo spazio delle possibili chiavi SSH, un attaccante potrebbe utilizzare un attacco di brute-force per provare tutte le combinazioni di chiavi pre-calcolate per ottenere l'accesso ai sistemi vulnerabili. Questo è particolarmente preoccupante su sistemi che utilizzano chiavi SSH compromesse per l'autenticazione.

3. **Falsificazione di Certificati SSL/TLS (Attacchi SSL/TLS)**: Le chiavi SSL/TLS generate utilizzando numeri casuali vulnerabili possono essere facilmente compromesse, consentendo a un attaccante di emettere certificati SSL/TLS falsificati per impersonare un server legittimo. Questo potrebbe portare a un attacco MITM, dove un attaccante si finge un server sicuro per raccogliere dati sensibili o per condurre attacchi più avanzati.
4. **Attacchi a DNSSEC (DNS Security Extensions)**: I DNSSEC usano chiavi crittografiche per garantire la sicurezza delle risposte DNS. Se un sistema vulnerabile generasse chiavi DNSSEC con numeri casuali prevedibili, un attaccante potrebbe generare falsi record DNS e manipolare il traffico, dirigendolo verso server compromessi.
5. **Falsificazione di Signatures Digitali (Attacchi DSA):** Poiché le chiavi DSA sono basate su numeri casuali utilizzati per la generazione di firme digitali, un attaccante potrebbe predire questi numeri e generare firme digitali falsificate. Questo compromette l'integrità delle comunicazioni e potrebbe permettere a un attaccante di ingannare sistemi di verifica
6. **Compromissione delle Sessioni Sicure (OpenVPN, X.509):** Anche le chiavi utilizzate in OpenVPN e per i certificati X.509 sono vulnerabili. Un attaccante potrebbe utilizzare una chiave compromessa per decrittografare traffico VPN sensibile o per impersonare un server durante una connessione SSL/TLS sicura.
7. **Exploit dei Vulnerabili Sistemi Debian Non Patched**: I sistemi che non sono stati aggiornati o che continuano a utilizzare le chiavi compromesse sono particolarmente vulnerabili. L'attaccante potrebbe approfittare della vulnerabilità per infiltrarsi in un sistema, aggirare meccanismi di autenticazione e ottenere privilegi elevati.

Conclusione sulle conseguenze degli attacchi:

1. **Compromissione della riservatezza**
2. **Accesso non autorizzato ai sistemi**
3. **Interruzione dei servizi**
4. **Falsificazione dei dati e delle comunicazioni**
5. **Compromissione della rete e della sicurezza aziendale**

Soluzione alla vulnerabilità:

La soluzione consiste nel rigenerare tutte le chiavi crittografiche generate con versioni vulnerabili di OpenSSL (a partire dalla versione 0.9.8c-1 su Debian) e considerare compromesse le chiavi DSA usate per firme o autenticazione. Anche altre vulnerabilità in OpenSSL, come problemi con la DTLS e attacchi tramite canalizzazioni laterali, saranno risolti.

Per correggere il problema:

1. Necessario **aggiornare il pacchetto OpenSSL** alla versione più recente disponibile e rigenerare il materiale crittografico.

- Per eseguire l'aggiornamento:

    Scarica il file: wget [url]

    Installa il pacchetto: dpkg -i file.deb

    Aggiornare il database interno: apt-get update

    Installazione dei pacchetti corretti: apt-get upgrade

E' anche possibile effettuare un aggiornamento automatizzato aggiungendo i seguenti pacchetti.

- **openssl_0.9.8c-4etch3_i386.deb**

Questo pacchetto contiene l'eseguibile principale di OpenSSL, inclusi gli strumenti a riga di comando per gestire certificati e operazioni di crittografia. È essenziale per garantire che le operazioni che dipendono da OpenSSL utilizzino una versione corretta e aggiornata.

Link:
http://security.debian.org/pool/updates/main/o/openssl/openssl_0.9.8c-4etch3_i386.deb

- **libssl0.9.8_0.9.8c-4etch3_i386.deb**

Questo pacchetto fornisce le librerie condivise necessarie per applicazioni che dipendono da OpenSSL (ad esempio, server web, client SSH, ecc.). È obbligatorio se il sistema utilizza applicazioni che richiedono questa libreria.

Link:
http://security.debian.org/pool/updates/main/o/openssl/libssl0.9.8_0.9.8c-4etch3_i386.deb

- **libssl-dev_0.9.8c-4etch3_i386.deb**

  Questo pacchetto include i file di sviluppo (header e altre risorse) per compilare applicazioni che usano OpenSSL. È necessario solo se hai bisogno di compilare software che dipende da OpenSSL.

  Link:
  http://security.debian.org/pool/updates/main/o/openssl/libssl-dev_0.9.8c-4etch3_i386.deb

2. Gli utenti verifichino le **chiavi SSH** vulnerabili tramite strumenti come il script Perl messo a disposizione da HD Moore, che permette di eseguire un attacco di brute-force per accedere ai sistemi vulnerabili.

   Un detector per individuare il materiale di chiavi deboli è disponibile a questo link:

   http://security.debian.org/project/extra/dowkd/dowkd.pl.gz

   http://security.debian.org/project/extra/dowkd/dowkd.pl.gz.asc (firma OpenPGP)

3. **Implementare il rollover delle chiavi** per vari pacchetti.

   http://www.debian.org/security/key-rollover/

   Sito in costante aggiornamento con nuove istruzioni sul rollover delle chiavi per i pacchetti che utilizzano certificati SSL, con l'elenco dei pacchetti popolari non interessati.

Mitigazione del rischio:

1. **Aggiorna OpenSSL** alla versione che include la correzione per la CVE-2008-0166.
2. **Disabilita MD5** e altri algoritmi di cifratura deboli nella configurazione SSL/TLS.
3. Verifica e testa la **configurazione SSL/TLS** per assicurarti che non vengano usati algoritmi vulnerabili.
4. Implementa pratiche di sicurezza aggiuntive come **HSTS e certificati validi** per proteggere il sistema da attacchi MITM.

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerabilities (USN-644-1)

CRITICAL	10.0*	6.7	0.8634	37936	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerabilitie (USN-644-1)

Descrizione vulnerabilità:

Libxml2, una libreria ampiamente utilizzata per l'elaborazione di documenti XML, è stata al centro di diverse vulnerabilità critiche che evidenziano i rischi associati alla gestione di dati non attendibili in ambienti software. Questi problemi sono particolarmente rilevanti per sistemi che si affidano a libxml2 per analizzare documenti XML provenienti da fonti esterne, dato che errori nella gestione delle entità XML possono portare a gravi conseguenze.

CVE-2008-3281 - Vulnerabilità di protezione nelle entità XML molto grandi che potrebbe causare l'attivazione errata di protezioni di vulnerabilità e il conseguente crash.

CVE-2008-3529 - Vulnerabilità nell'elaborazione dei nomi delle entità in libxml2. Libxml2 non gestisce correttamente i nomi delle entità XML

Possibili rischi di attacchi:

1. **Esecuzione di codice arbitrario:** Un attaccante può sfruttare vulnerabilità come l'overflow del buffer basato su heap per inserire ed eseguire codice arbitrario sul sistema vittima. Così facendo può ottenere lo stesso livello di accesso dell'applicazione vulnerabile e può installare malware, rubare dati sensibili o assumere il controllo del sistema.

2. **Denial of Service (DoS):** Questi attacchi sfruttano problemi come la gestione ricorsiva delle entità XML o i nomi di entità estremamente lunghi per sovraccaricare il sistema. Questo causerà consumo eccessivo di risorse (CPU e memoria), causando rallentamenti o crash del sistema.

3. **XML External Entity (XXE):** Una cattiva gestione delle entità XML in libxml2 può esporre al rischio di un attacco XXE. Questo attacco sfrutta entità esterne definite nei documenti XML per accedere a file locali o inviare dati sensibili a server remoti. Causando esfiltrazione di file sensibili dal server (es. chiavi di configurazione, password).
   Esempio: Un documento XML include un'entità che punta a un file locale (/etc/passwd). Quando il parser lo elabora, invia il contenuto del file a un server remoto controllato dall'attaccante.

4. **Bypass delle protezioni di sicurezza:** Le vulnerabilità possono essere utilizzate per eludere le misure di sicurezza introdotte in patch precedenti, come nel caso di USN-640-1, che non gestiva correttamente documenti XML con entità valide ma molto grandi.

5. **RCE (Remote Code Execution) mirato:** Un attaccante esperto può combinare vulnerabilità come l'overflow del buffer con altre debolezze presenti nell'applicazione o nel sistema operativo per eseguire codice dannoso in remoto. Questo genere di attacco potrebbe portare alla compromissione totale degli interi sistemi, utilizzando il sistema compromesso come punto di partenza per attacchi a catena verso altri sistemi nella rete.

Conclusione sulle conseguenze degli attacchi:

1. **Compromissione della sicurezza** (Accesso non autorizzato ed esecuzione di codice arbitrario)
2. **Interruzione del servizio** (Denial of Service, DoS)
3. **Furto o esposizione di dati sensibili** (Esfiltrazione di dati)
4. **Escalation dei privilegi** (Aumento del controllo sul sistema)
5. **Danno alla reputazione e perdita di fiducia**
6. **Conseguenze finanziarie**
7. **Compromissione di altre risorse o reti (Attacchi a catena)**
8. **Spionaggio o sabotaggio**
9. **Implicazioni legali e normative**
10. **Obblighi di notificare le violazioni**

Le vulnerabilità in libxml2 possono avere un impatto devastante, sia in termini di sicurezza che di affidabilità del sistema. Un attacco può portare a compromissioni dirette, come l'esecuzione di codice arbitrario o il furto di dati, e a conseguenze indirette, come danni reputazionali, legali e finanziari.

Soluzioni alla vulnerabilità:

Per risolvere le vulnerabilità CVE-2008-3281 e CVE-2008-3529 in libxml2, è necessario applicare aggiornamenti e patch specifici.

1. **CVE-2008-3281** - Vulnerabilità di protezione nelle entità XML molto grandi che potrebbe causare l'attivazione errata di protezioni di vulnerabilità e il conseguente crash.
2. **CVE-2008-3529** - Vulnerabilità nell'elaborazione dei nomi delle entità in libxml2. Libxml2 non gestisce correttamente i nomi delle entità XML.

   Aggiornamento a una versione sicura di libxml2. Ubuntu ha rilasciato una patch con USN-640-1 per risolvere questa vulnerabilità. La soluzione consiste nell'aggiornare libxml2 alla versione più recente disponibile nel repository ufficiale di Ubuntu.

   Per eseguire l'aggiornamento: sudo apt upda

   sudo apt upgrade libxml2

   Verifica che la versione di libxml2 sia aggiornata: dpkg -l | grep libxml2

   La versione deve essere almeno la 2.6.32 o successiva

   Aggiorna il sistema: sudo apt update

   sudo apt upgrade

Oppure compilare manualmente da sorgenti:

- Scaricare l'ultima versione di libxml2 dal sito ufficiale o dai repository di codice.

  Compilare e installare la nuova versione: ./configure

  make

  sudo make install

  Verificare l'installazione: xml2-config --version

Mitigazione del rischio:

Per mitigare questi rischi, è essenziale adottare una serie di misure.

1. Prima di tutto, mantenere sempre **aggiornate le librerie software** è fondamentale.
2. In ambienti particolarmente sensibili, come server o applicazioni esposte a Internet, l'utilizzo di tecniche di isolamento può aiutare a contenere i danni in caso di attacco. Ad

esempio, eseguire l'applicazione in un ambiente sandbox può limitare i privilegi del processo e impedire che un attacco porti alla compromissione dell'intero sistema.

3. L'adozione di misure di sicurezza come il monitoraggio delle risorse, il controllo degli input e la protezione della memoria può ulteriormente ridurre il rischio associato a queste vulnerabilità.
