# Report vulnerabilità

# Per questo esercizio mi sono concentrato principalmente sulle vulnerabilità critiche, che, come visto dallo scan effettuato, si sono rivelate essere 3.

# SSL Version 2 and 3 Protocol Detection

## 1. Motivo della Criticità

La vulnerabilità SSL Version 2 and 3 Protocol Detection, con un punteggio di CVSS 9.8 (CRITICAL), indica che il server target supporta ancora i protocolli di sicurezza SSLv2 e/o SSLv3. Questi protocolli sono considerati gravemente insicuri e soggetti a molteplici vulnerabilità, rendendo il sistema potenzialmente esposto ad attacchi critici.  
  
SSLv2: È estremamente vecchio e presenta difetti di progettazione, tra cui la mancanza di forward secrecy e chiavi crittografiche deboli.  
SSLv3: Sebbene migliore di SSLv2, è vulnerabile a diversi attacchi noti, in particolare:  
- Attacco POODLE (Padding Oracle On Downgraded Legacy Encryption): Permette a un attaccante di decifrare i dati criptati.  
- Mancanza di supporto per algoritmi di crittografia moderni.  
- Nessun supporto per suite di cifratura resistenti agli attacchi attuali.

## 2. Implicazioni

- Esposizione a dati sensibili: Le connessioni potrebbero essere decifrate o alterate da un attaccante.  
- Compliance Issues: L'uso di SSLv2 o SSLv3 non è conforme agli standard di sicurezza moderni come PCI DSS, HIPAA, e NIST.  
- Facilità di exploit: Gli strumenti per sfruttare queste vulnerabilità sono ampiamente disponibili.

## 3. Risoluzione

Per mitigare questa vulnerabilità, è necessario disabilitare il supporto per SSLv2 e SSLv3 nel server target.

## 4. Consigli

- Abilita solo protocolli moderni (TLSv1.2 e TLSv1.3).  
- Configura suite di cifratura sicure (escludi cifre deboli come RC4 o 3DES).  
- Monitora regolarmente le configurazioni di sicurezza del server.

# Debian OpenSSH/OpenSSl Package Random Number Generator Weakness

La vulnerabilità **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness** (spesso nota come **Debian OpenSSL RNG Issue**) è una delle vulnerabilità critiche legate alla generazione di numeri casuali nel pacchetto OpenSSL fornito da Debian.

**1. Descrizione della Vulnerabilità**

La vulnerabilità (CVE-2008-0166) è stata introdotta nelle versioni modificate di OpenSSL distribuite nei pacchetti Debian e derivati (es. Ubuntu) tra il 2006 e il 2008. Un cambiamento errato nel codice ha ridotto drasticamente l'entropia utilizzata per generare numeri casuali, compromettendo la sicurezza crittografica e generando chiavi deboli.

* **Impatto principale**: Chiavi crittografiche generate su sistemi vulnerabili hanno un'entropia estremamente bassa e sono facilmente prevedibili.
* **Componenti affetti**: Include chiavi SSH, certificati SSL/TLS e chiavi utilizzate in VPN o altre applicazioni crittografiche.

**2. Implicazioni**

* **Severità (CVSS 10.0)**: Critico, in quanto le chiavi generate su sistemi vulnerabili possono essere brute-forzate con facilità.
* **Esposizione**:
  + Attaccanti remoti possono calcolare le chiavi private corrispondenti alle chiavi pubbliche generate.
  + Intercettazione e decrittazione delle comunicazioni crittografate (MITM).
  + Accesso non autorizzato a server SSH e altri sistemi crittografici.
* **Impatto su sistemi Debian e derivati**: Sistemi affetti che hanno generato chiavi durante il periodo vulnerabile rimangono compromessi, anche se successivamente aggiornati.

**3. Prevenzione**

1. **Configurazione robusta**:
   * Evita modifiche arbitrarie ai pacchetti di sicurezza critici come OpenSSL.
   * Utilizza repository di pacchetti ufficiali.
2. **Monitoraggio continuo**:
   * Esegui scansioni periodiche per rilevare chiavi deboli o configurazioni vulnerabili.
3. **Verifica di sicurezza aggiuntiva**:
   * Adotta strumenti di analisi della sicurezza per controllare le chiavi e configurazioni crittografiche.

**6. Consigli**

* Mantieni il software di sicurezza aggiornato.
* Usa protocolli crittografici moderni come **TLSv1.2** e **TLSv1.3**.
* Configura il server per disabilitare cifre e protocolli deboli.
* Implementa politiche di gestione delle chiavi che includano revisione e rotazione periodica.

Questa vulnerabilità è un esempio emblematico di come errori apparentemente minori nella gestione del software crittografico possano avere un impatto devastante sulla sicurezza dei sistemi. La mitigazione e la rigenerazione tempestiva delle chiavi sono essenziali per eliminare i rischi associati.