REPORT Vulnerabilità Critiche

Vulnerabilità Critica: Debolezza nel Generatore di Numeri Casuali di OpenSSL su Debian (CVE-2008-0166)

Descrizione: Un certificato SSL/TLS presente sul server remoto è stato generato su un sistema Debian o Ubuntu affetto da un bug critico nel generatore di numeri casuali di OpenSSL. Questo bug, introdotto durante il processo di packaging Debian, ha rimosso quasi tutte le fonti di entropia necessarie per generare chiavi crittograficamente sicure. Di conseguenza, la chiave privata associata al certificato è facilmente prevedibile e può essere ottenuta da un attaccante.

Impatto:

- **Compromissione della riservatezza e integrità dei dati:** Un attaccante può decifrare il traffico HTTPS protetto dal certificato vulnerabile, esponendo informazioni sensibili come credenziali di accesso, dati personali o transazioni finanziarie.
- **Attacchi Man-in-the-Middle:** L'attaccante può impersonare il server legittimo, intercettando e manipolando le comunicazioni tra il client e il server.

Soluzione:

- **Considerare compromesso tutto il materiale crittografico generato sull'host remoto.** In particolare, tutte le chiavi SSH, SSL e OpenVPN dovrebbero essere rigenerate.

Vulnerabilità: Utilizzo di protocolli SSL/TLS obsoleti (SSL 2.0 e 3.0)

Descrizione: Il servizio remoto accetta connessioni che utilizzano i protocolli SSL 2.0 e/o SSL 3.0, entrambi considerati insicuri a causa di diverse vulnerabilità crittografiche note. Queste vulnerabilità possono consentire ad un attaccante di eseguire attacchi man-in-the-middle o decifrare le comunicazioni tra il servizio e i suoi client.

Impatto:

- **Compromissione della riservatezza:** Possibilità di intercettazione e decifrazione del traffico dati, esponendo informazioni sensibili.
- **Attacchi Man-in-the-Middle:** Possibilità di interposizione di un attaccante nella comunicazione, consentendo la manipolazione o l'alterazione dei dati scambiati.

Soluzione:

- **Disabilitare SSL 2.0 e 3.0:** Consultare la documentazione dell'applicazione per disabilitare questi protocolli obsoleti.
- **Utilizzare TLS 1.2 o superiore:** Configurare il servizio per utilizzare esclusivamente TLS 1.2 o versioni successive, assicurandosi di selezionare suite di cifratura robuste e approvate.