Critical

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

Questa vulnerabilità riguarda un problema nei pacchetti OpenSSH/OpenSSL su sistemi Debian o Ubuntu. Dato che il certificato SSL  è stato generato su uno di questi sistemi e presenta una vulnerabilità nel generatore casuale di numeri della libreria OpenSSL perciò si verifica un problema derivante dalla rimozione di quasi tutte le fonti di casualità da parte di un pacchettizzatore Debian nella versione remota di OpenSSL.

In pratica, ciò significa che un attaccante potrebbe facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o effettuare un attacco man-in-the-middle.

**Soluzione**
Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

Critical

**Bind Shell Backdoor Detection**

Questa vulnerabilità riguarda la rilevazione di una "Bind Shell Backdoor" cioè un tipo specifico di backdoor che crea una shell (interfaccia da linea di comando) su una porta remota, senza richiedere autenticazione, offrendo così un accesso diretto al sistema per l'attaccante.

**Soluzione**
Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

High

**rlogin Service Detection**

Questa vulnerabilità riguarda il servizio rlogin su un host remoto. I dati inviati tra il client e il server rlogin  non sono crittografati, quindi consentono a un potenziale attaccante di intercettare informazioni sensibili. Il servizio potrebbe anche permettere accessi poco autenticati (senza password), presentando ulteriori rischi. Questo caso presenta svariate opportunità di attacco e compromissione del sistema.

**Soluzione**
Commentare la riga 'login' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare questo servizio e utilizzare invece SSH.