Ricerca vulnerabilità trovate con Nessus

Cache poisoning: si verifica quando gli aggressori manipolano le cache DNS per reindirizzare gli utenti a siti Web dannosi inserendo falsi record DNS nella cache. Il campo ID query è un componente cruciale nella prevenzione di tali attacchi, poiché aggiunge casualità alle query DNS, rendendole più difficili da prevedere e manipolare per gli aggressori.

ICMP Timestamp Request Remote Date Disclosure: l'host remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un utente malintenzionato di conoscere la data impostata sulla macchina presa di mira, il che può aiutare un utente malintenzionato remoto non autenticato a sconfiggere i protocolli di autenticazione basati sul tempo.

libndp >= 1.0 Buffer Overflow: Questo difetto consente a un utente malintenzionato locale di causare un buffer overflow in NetworkManager, attivato dall'invio di un pacchetto pubblicitario del router IPv6 non valido. Questo problema si è verificato poiché libndp non convalidava correttamente le informazioni sulla lunghezza del percorso.

SSL Certificate Cannot Be Trusted: Se l'host remoto è un host pubblico, qualsiasi interruzione nella catena rende più difficile per gli utenti verificare l'autenticità e l'identità del server web. Ciò potrebbe rendere più semplice l'esecuzione di attacchi man-in-the-middle contro l'host remoto.

Apache Tomcat AJP Connector Request Injection (Ghostcat): È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non

autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice in modalità remota (RCE).

Bind Shell Backdoor Detection: Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness: Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle.

VNC Server 'password' Password: Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.