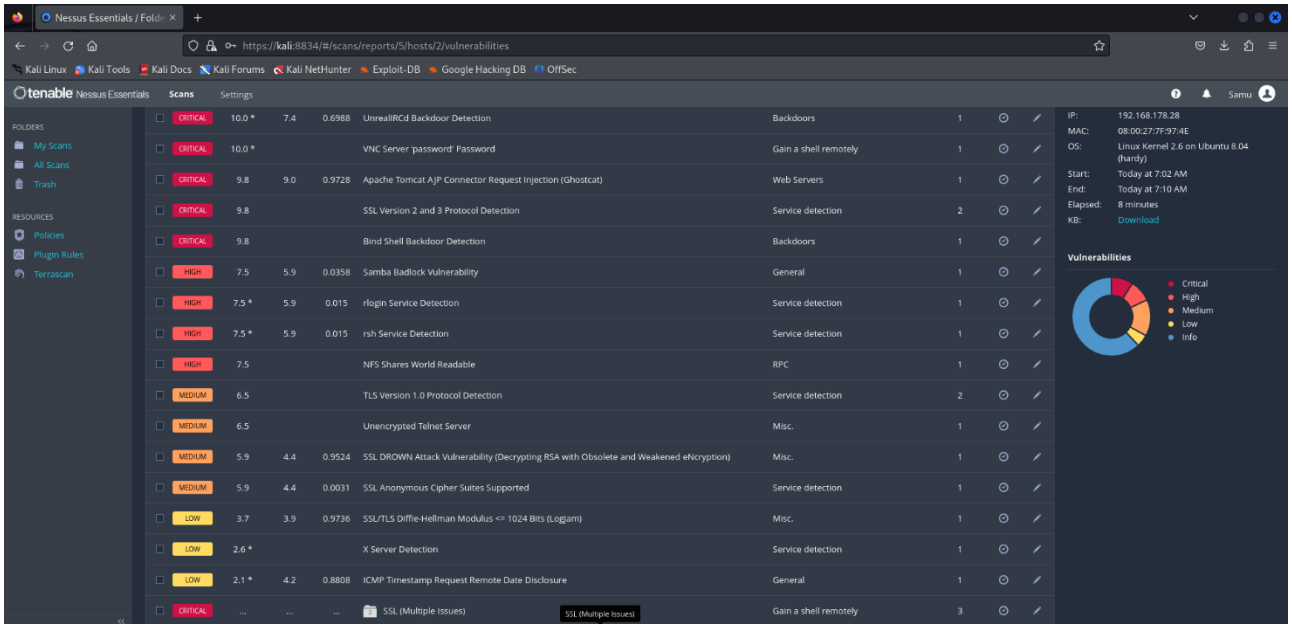
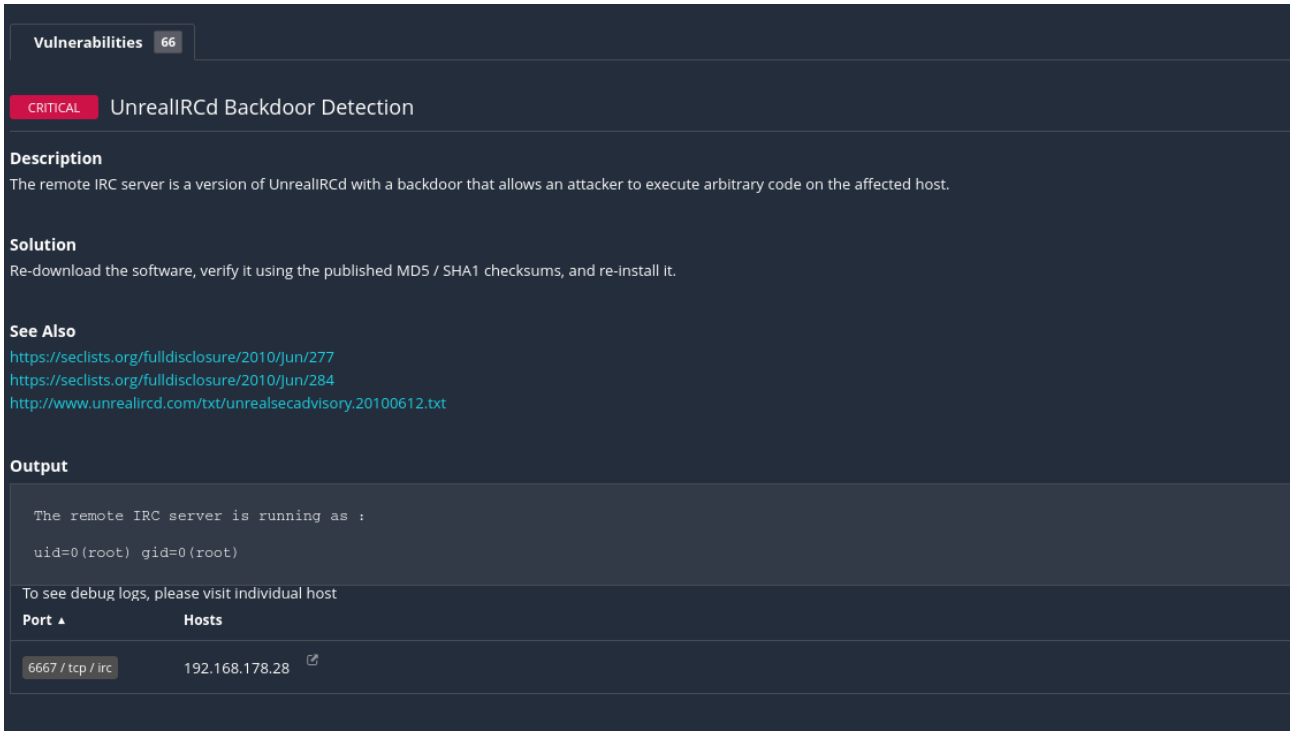
NESSUS

Nell'esercizio odierno è stato studiato il funzionamento del software Nessus, tool che fornisce informazioni soggettive in grado di effettuare, dato un indirizzo IP, con il quale la nostra macchina sia comunicante, un ping, invierà pacchetti TCP con la TWH completa, in modo da scansionare le porte aperte, SO e registri, ed infine proverà tramite diversi exploit ad attaccare la macchina.

Al fine di prendere confidenza con il software in questione, è stato effettuato uno scan sulla macchina vulnerabile Metasploitable 2. Dopo un po' di tempo il software ha fornito come risultati 9 vulnerabilità critiche, nonché altre vulnerabilità più o meno gravi. In seguito alla scansione sono state fornite ulteriori informazioni sulle vulnerabilità trovate, spiegando nel dettaglio come sia stato possibile sfruttarle e le possibili soluzioni per limitare il problema, stilando in totale 4 report differenti.

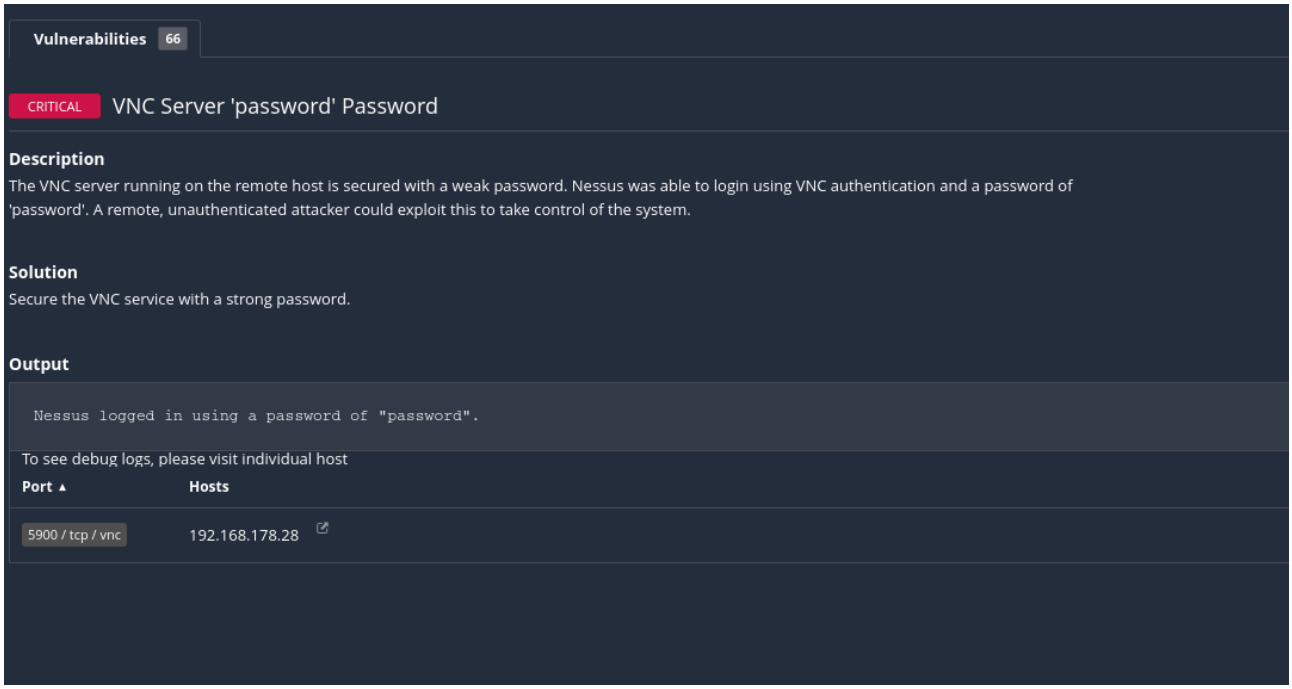




UnreallRCD

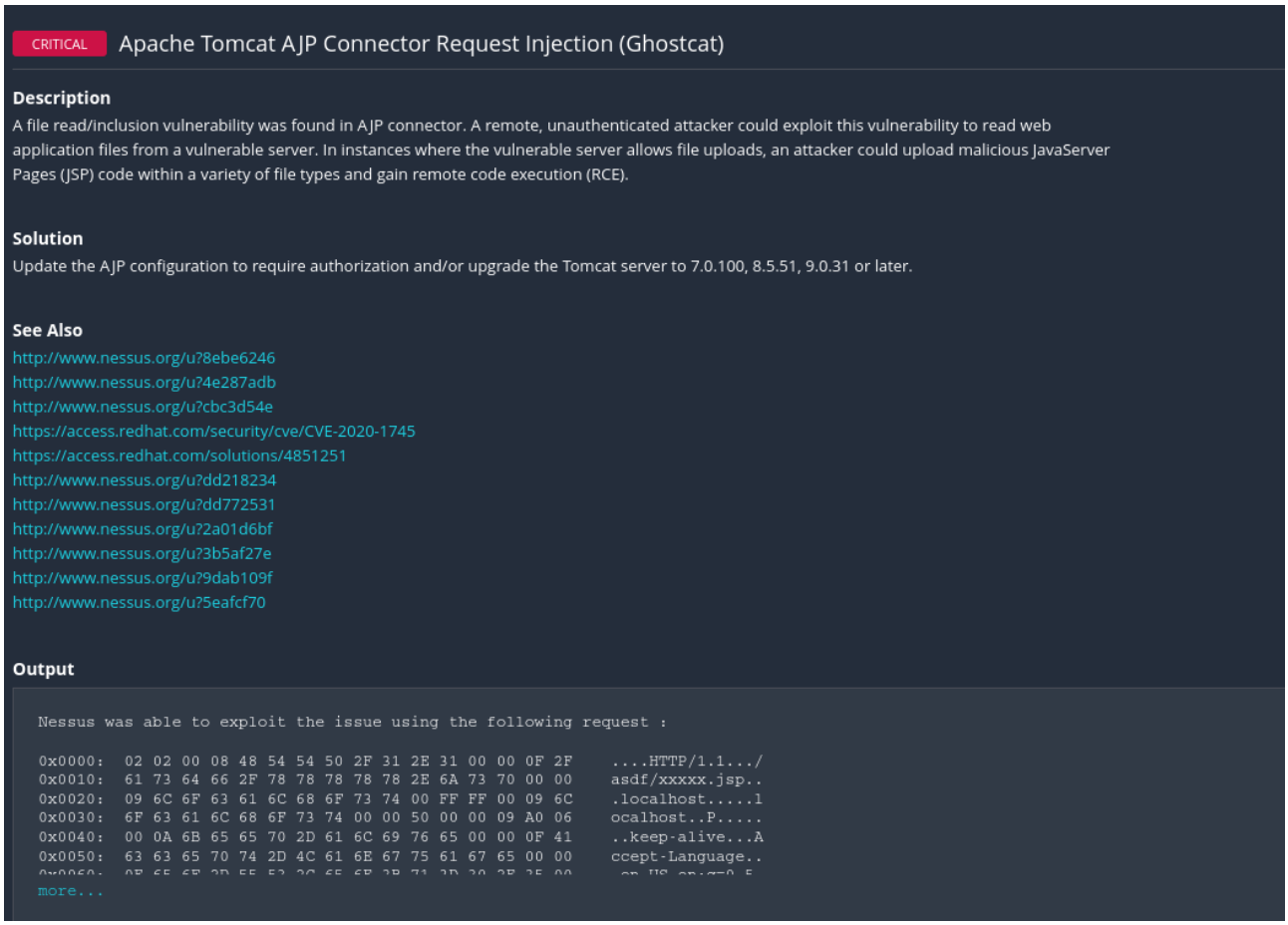
In modo particolare è stata inoltre effettuata una ricerca, nonché analisi in articolare su 5 vulnerabilità critiche. La prima è una vulnerabilità relativa alla UnreeallRCD Backdoor, in cui se ci si informa sui link forniti da Nessus ci dirà che “Abbiamo scoperto che il file Unreal3.2.8.1.tar.gz sui nostri mirror è stato sostituito qualche tempo fa con una versione dotata di backdoor (trojan). Questa backdoor consente a una persona di eseguire QUALSIASI comando con il file privilegi dell'utente che esegue l'ircd. La backdoor può essere eseguita indipendentemente da qualsiasi utente restrizioni”. In seguito a questa informazione viene suggerita una soluzione, quale re-installare il software, verificandone l’integrità e scaricarlo.

VNC SERVER vulnerability



La seconda vulnerabilità critica riguarda la password della macchina vulnerabile, in modo particolare la password base per quanto riguarda la sicurezza del VNC Server (Virtual Network Computing), la quale è stata facilmente bypassata dal software Nessus senza alcun problema. Come soluzione sarebbe opportuno cambiare la password in una molto più efficace.

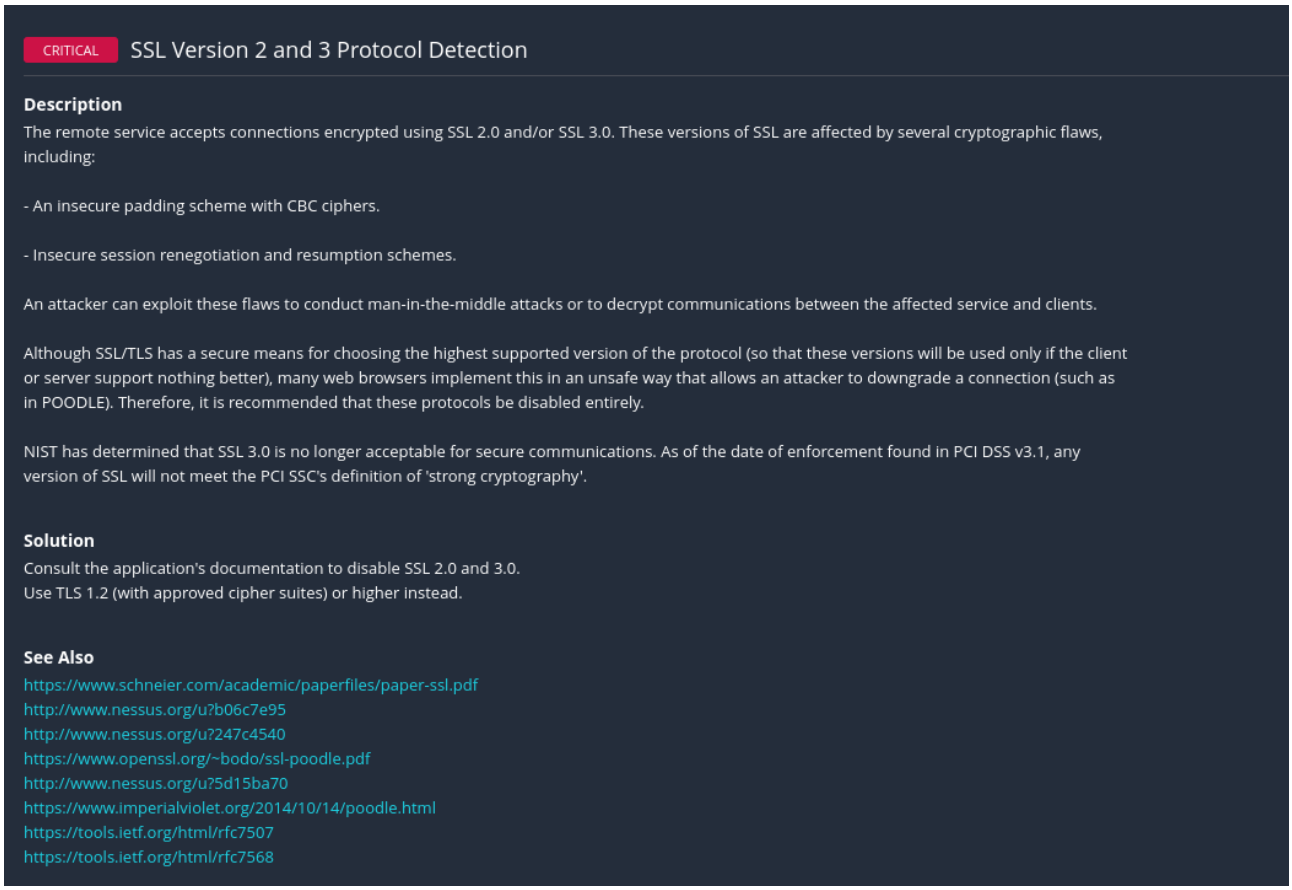
APACHE Tomcat AJP



La terza vulnerabilità critica trovata riguarda Apache. Nessus ci dice che è presente un file read/inclusion nel connettore AJP, un protocollo binario che può inoltrare richieste in entrata da un server Web a un server delle applicazioni che si trova dietro il server Web. Ci dice inoltre che un attaccante senza shell privilegiata potrebbe utilizzarlo per poter leggere i file dell'applicazione web da un server vulnerabile, oppure, in caso sia consentito l'upload dei file, di caricare pagine malevole con lo scopo di inserire codice malevolo ed ottenere l'RCE remote code execution. Nei link sotto riportati sono elencate tutte le vulnerabilità delle varie versioni con le possibili soluzioni per mitigare il problema.

Inseguito come soluzione ci viene proposto di fare un update alla configurazione del protocollo AJP in modo che sia accessibile solo a chi abbia l'autorizzazione e/o di aggiornare il server Tomcat alle versioni più recenti.

SSL v2/3 e Protocol Detection



CRITICAL SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

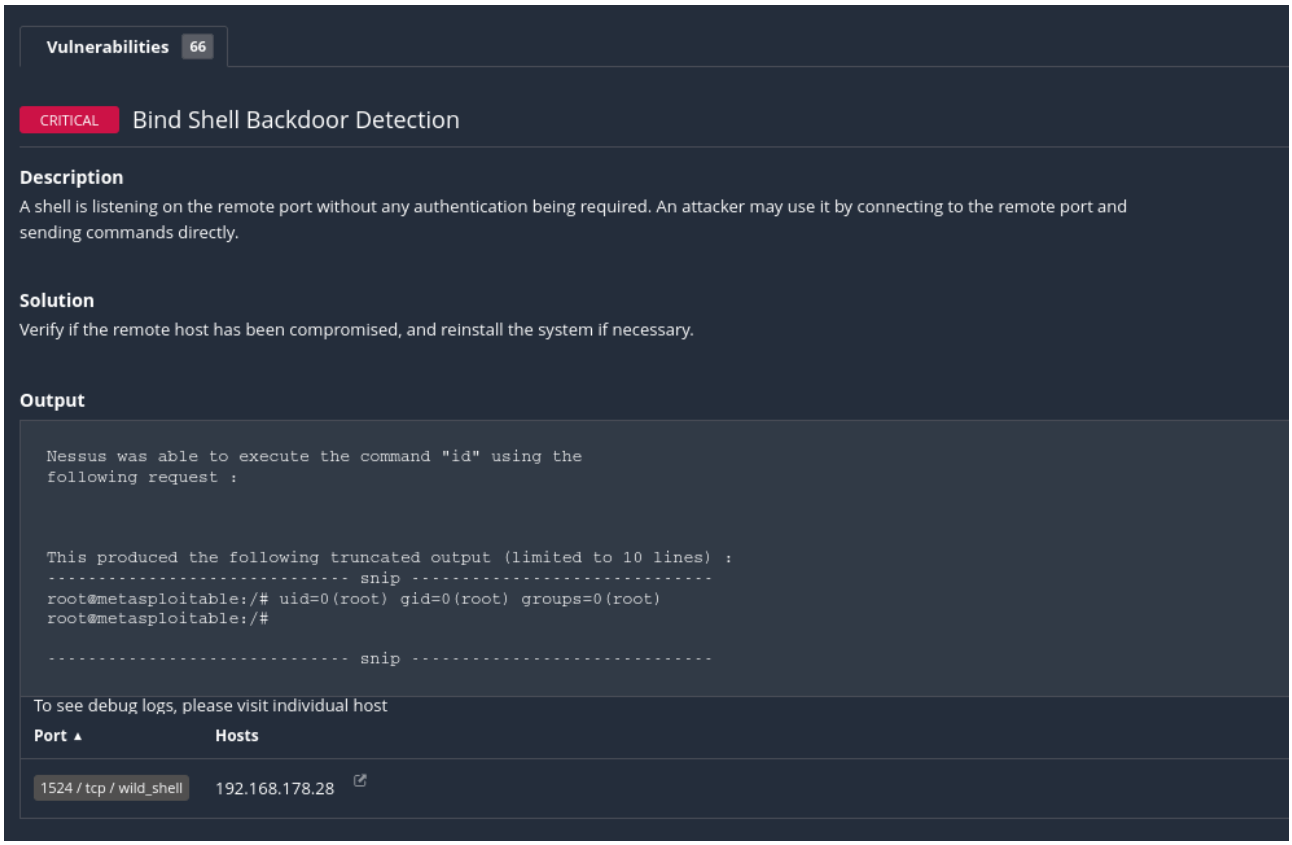
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

Come quarta vulnerabilità analizzata, avremo due versioni di SSL, una tipologia di crittografia, spiegando che il servizio di accesso remoto utilizza delle versioni di quest'ultima che peccano di cryptografic flaws, ovvero hanno delle screpolature nella crittografia utilizzata. A causa di queste screpolature un possibile man in the middle potrebbe sniffare i dati decriptando eventuali comunicazioni in atto. Le versioni di SSL e TLS vengono solitamente "scelte" alla versione più aggiornata, ma solo se supportate dal client o dal server, in caso contrario verrà utilizzata la versione precedente. Come soluzione, siccome le nuove versioni possono non essere supportate, ci viene suggerito di disabilitare le due versioni di SSL, tramitee un procedimento documentato dai link forniti dal software, ed utilizzare TLS 1.2 o +.

Bind Shell Backdoor



Come quinta vulnerabilità è stato rilevata una shell in ascolto su una porta in remoto, senza alcuna autorizzazione. Potrebbe essere sfruttata per inviare direttamente comandi sulla macchina vulnerabile, ragion per cui ci viene suggerito di verificare se l'host remoto sia stato compromesso, e se necessario, re installare il sistema.