SCANSIONE NESSUS METASPLOITABLE (*COMMON PORTS)*

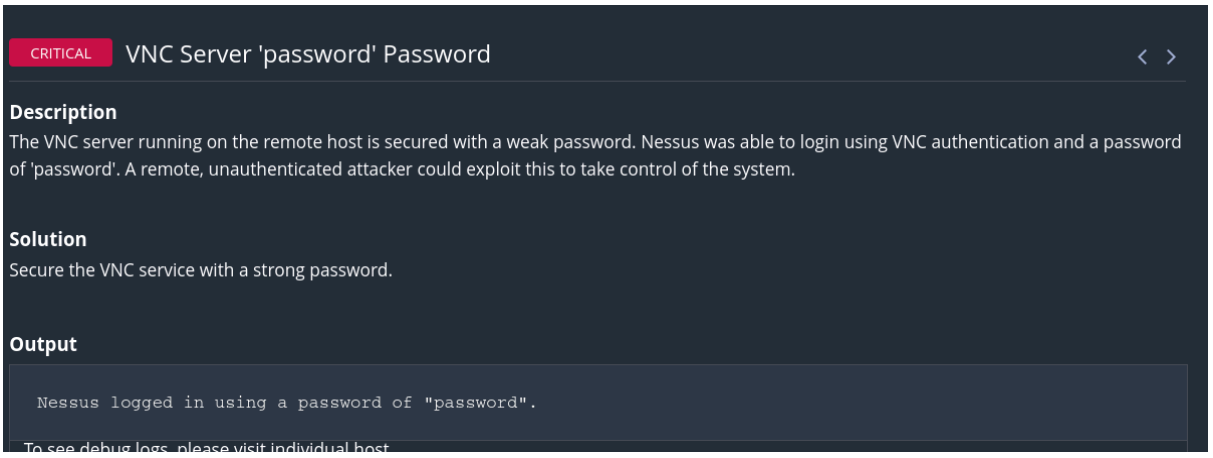
Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *			VNC Server 'pass...	Gain a shell remotely	1
CRITICAL	9.8	9.0	0.9737	Apache Tomcat ...	Web Servers	1
CRITICAL	9.8			SSL Version 2 an...	Service detection	2
CRITICAL	9.8			Bind Shell Backd...	Backdoors	1
CRITICAL	...	...	...	SSL (Multipl...	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	Samba Badlock ...	General	1
HIGH	7.5			NFS Shares Worl...	RPC	1
MIXED	...	...	...	SSL (Multipl...	General	28
MIXED	...	...	...	ISC Bind (M...	DNS	5
MEDIUM	6.5			TLS Version 1.0 ...	Service detection	2

Host Details

IP:	192.168.50.101
MAC:	08:00:27:6E:DF:86
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 2:13 PM
End:	Today at 2:38 PM
Elapsed:	24 minutes
KB:	Download

Vulnerabilities

1. CRITICITA’ 10 password debole



CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

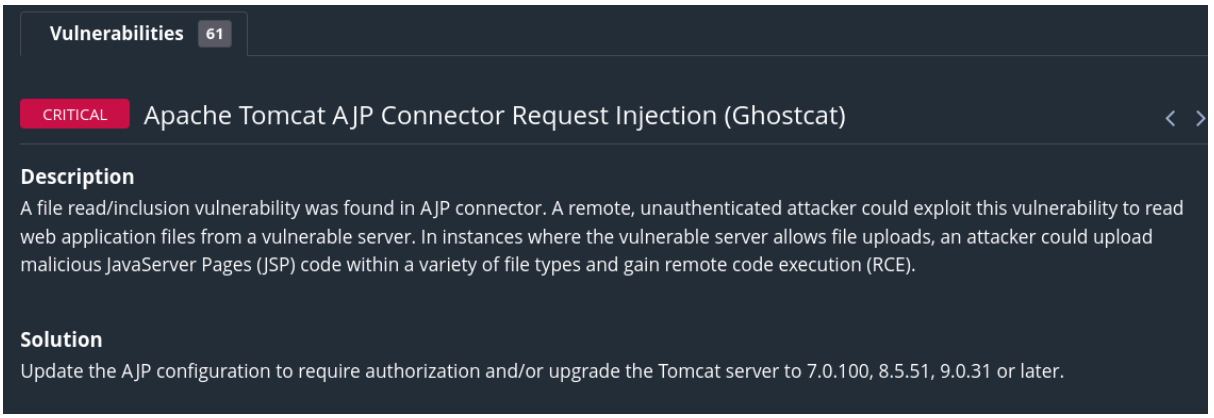
Output

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

E’ stata rilevata una vulnerabilità dal fatto che la password è salvata come “password”.

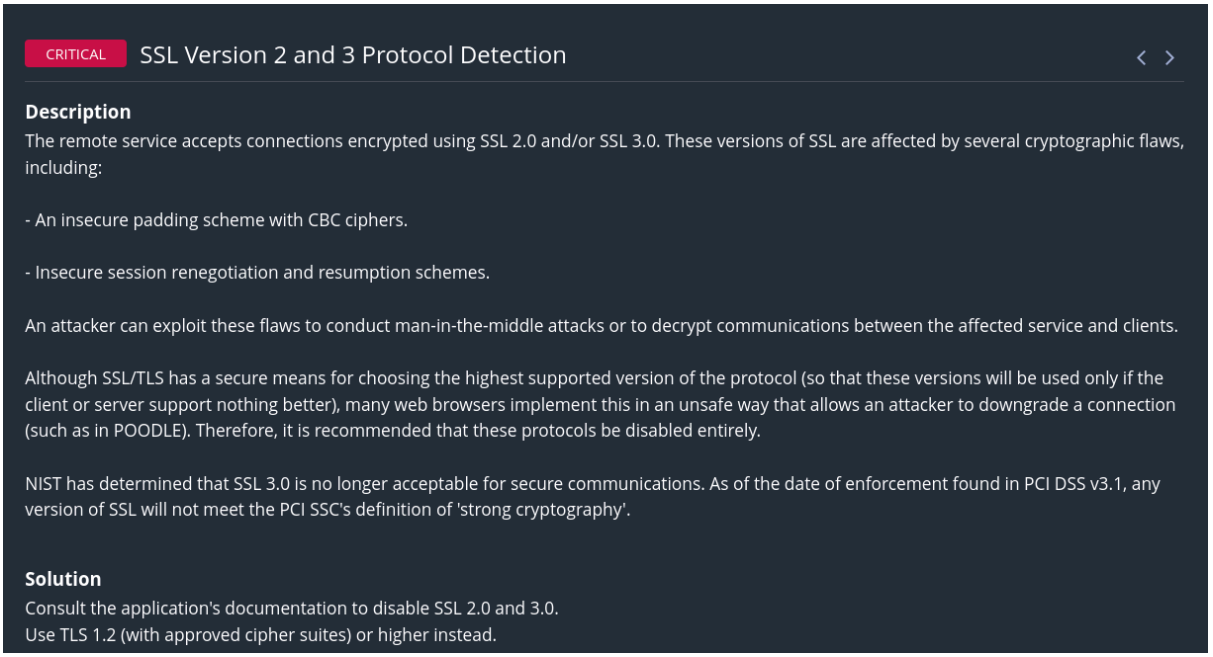
2. CRITICITA’ 9.8 Ghostcat



È stata trovata una vulnerabilità nel connettore AJP di Apache Tomcat, chiamata *Ghostcat*. Questa vulnerabilità permette a un attaccante remoto e non autenticato di leggere file delle applicazioni web dal server vulnerabile. Se il server consente il caricamento di file, l'attaccante potrebbe caricare codice JSP malevolo e ottenere l'esecuzione di codice remoto (RCE).

Soluzione
Aggiorna la configurazione del connettore AJP per richiedere l'autenticazione e/o aggiorna il server Tomcat alle versioni 7.0.100, 8.5.51, 9.0.31 o successive.

3. CRITICITA’ 9.8 Servizi ssl obsoleti



Descrizione
Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0, versioni affette da diverse vulnerabilità crittografiche, tra cui:

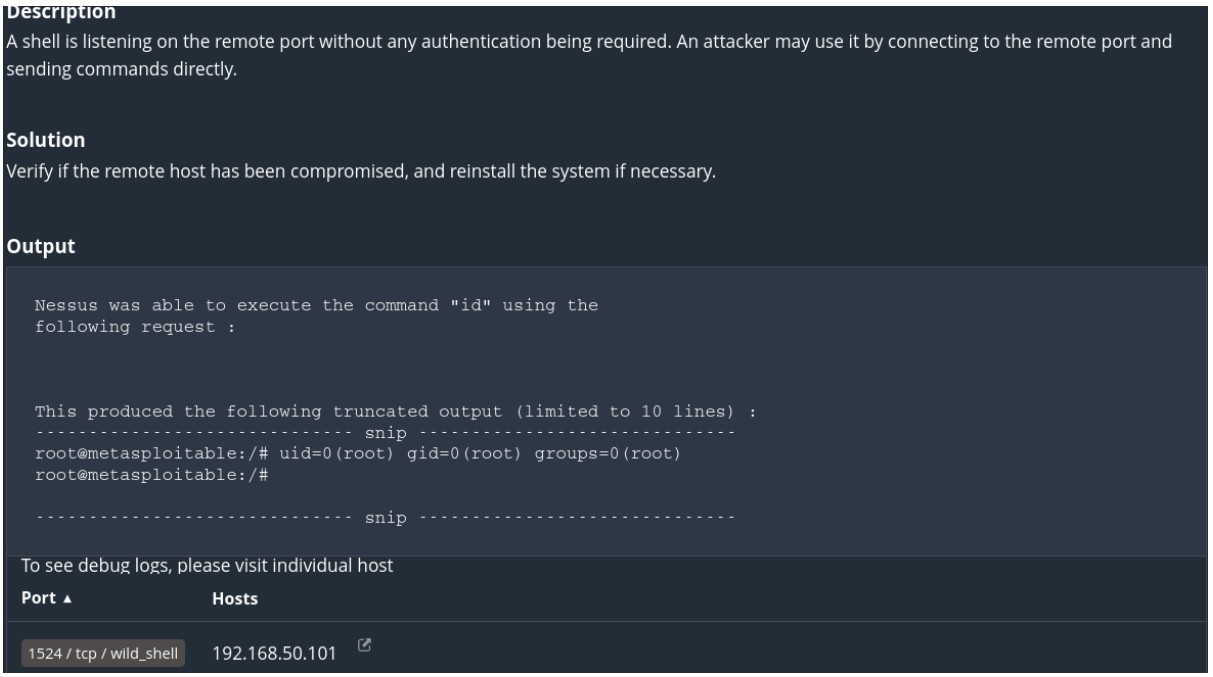
- Schema di padding insicuro con cifrari CBC.
- Schemi insicuri di rinegoziazione e ripresa delle sessioni.

Un attaccante può sfruttare queste falle per condurre attacchi *man-in-the-middle* o decriptare le comunicazioni tra il servizio e i client.

Questi protocolli sono considerati obsoleti, e i browser possono consentire downgrade delle connessioni, come nell'attacco POODLE. Per questo motivo, si consiglia di disabilitare completamente SSL 2.0 e 3.0. NIST ha dichiarato SSL 3.0 inaccettabile per comunicazioni sicure, e secondo PCI DSS v3.1 nessuna versione di SSL è considerata crittografia forte.

Soluzione
Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizza TLS 1.2 (o versioni superiori) con suite di cifratura approvate.

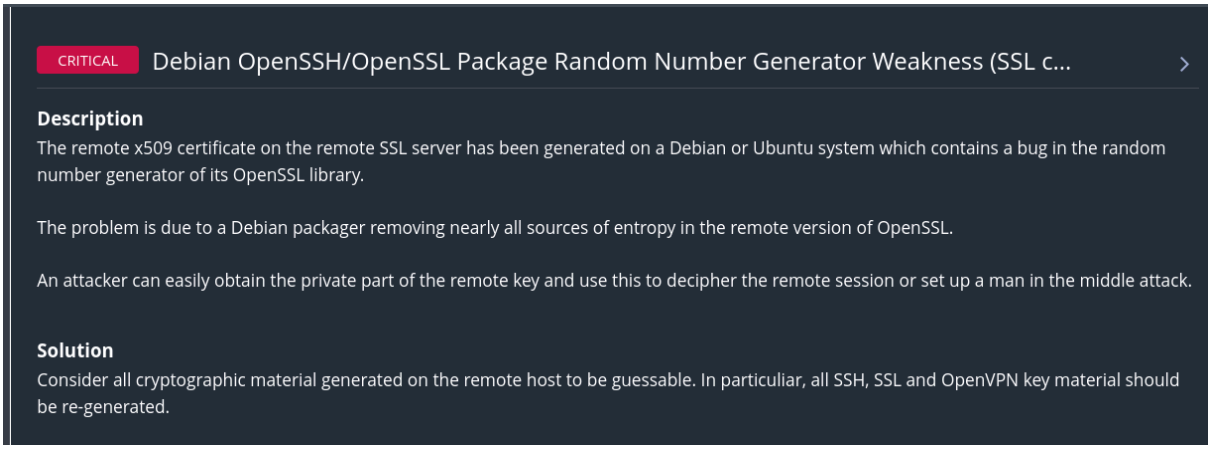
4. CRITICITA’ 9.8 Backdoor



Descrizione
Una shell è in ascolto su una porta remota senza richiedere alcuna autenticazione. Un attaccante potrebbe sfruttarla connettendosi alla porta remota ed eseguendo comandi direttamente.

Soluzione
Verifica se l'host remoto è stato compromesso e, se necessario, reinstalla il sistema.

5. **CRITICITA' 9.8 Certificato x509 weak**



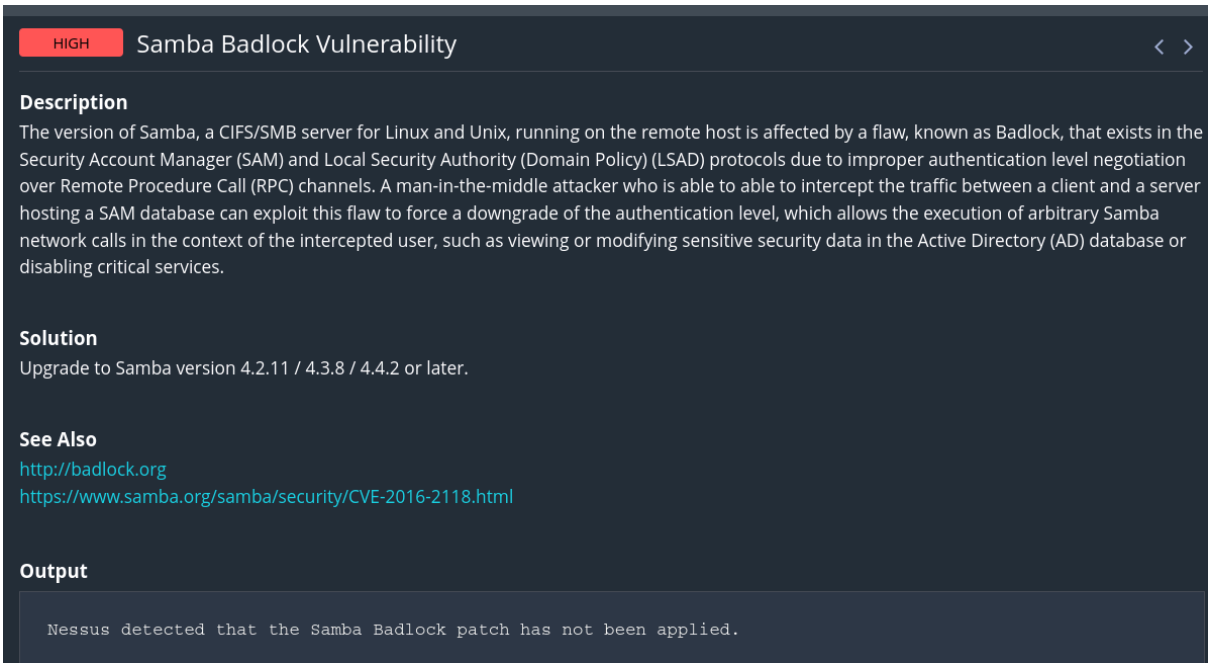
Descrizione
Il certificato x509 usato dal server SSL remoto è stato creato su un sistema Debian o Ubuntu con una versione di OpenSSL affetta da un grave difetto nel generatore di numeri casuali.

Questo problema deriva da una modifica apportata ai pacchetti Debian che ha eliminato quasi tutte le fonti di casualità, rendendo le chiavi generate prevedibili.

Di conseguenza, un attaccante potrebbe ricavare facilmente la chiave privata del server, consentendo di intercettare e decifrare le comunicazioni o di simulare il server per attacchi *man-in-the-middle*.

Soluzione
Tutte le chiavi crittografiche generate sull'host (incluse quelle per SSH, SSL e OpenVPN) devono essere rigenerate, perché sono da considerarsi insicure.

6. **CRITICITA’ 7.5 Samba badlock**

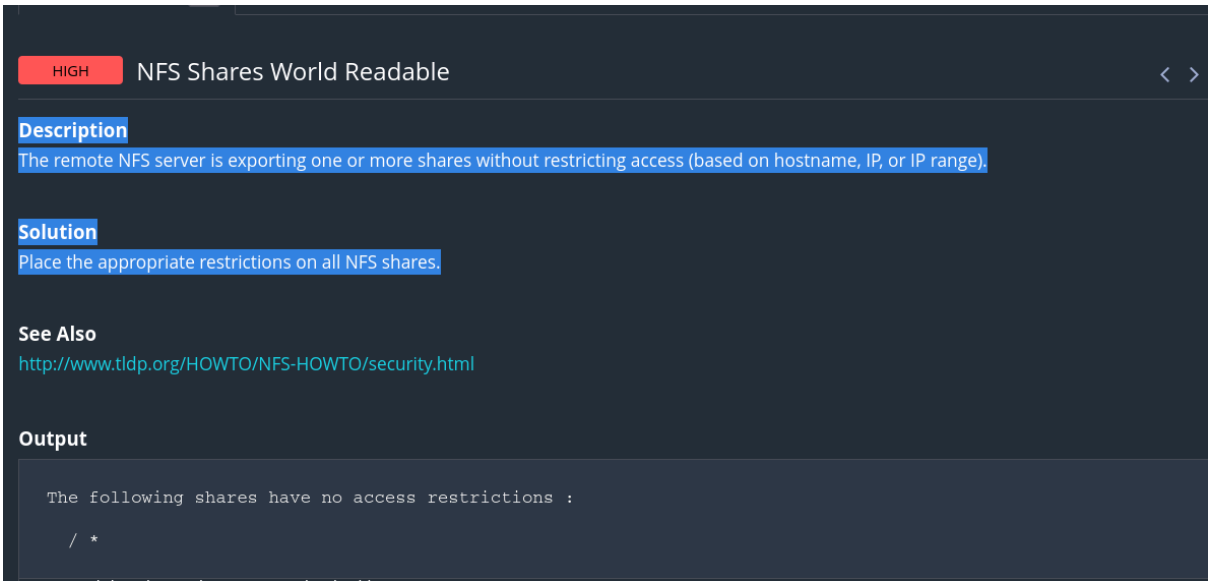


Descrizione
La versione di Samba in esecuzione sull'host remoto è vulnerabile a un difetto noto come *Badlock*. Questo problema riguarda i protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione inadeguata del livello di autenticazione nei canali di chiamata di procedura remota (RPC).

Un attaccante *man-in-the-middle* che intercetta il traffico tra un client e un server con un database SAM può sfruttare questa vulnerabilità per forzare un downgrade del livello di autenticazione. Questo gli consente di eseguire chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza in Active Directory (AD) o disabilitare servizi critici.

Soluzione
Aggiorna Samba alla versione 4.2.11, 4.3.8, 4.4.2 o successiva.

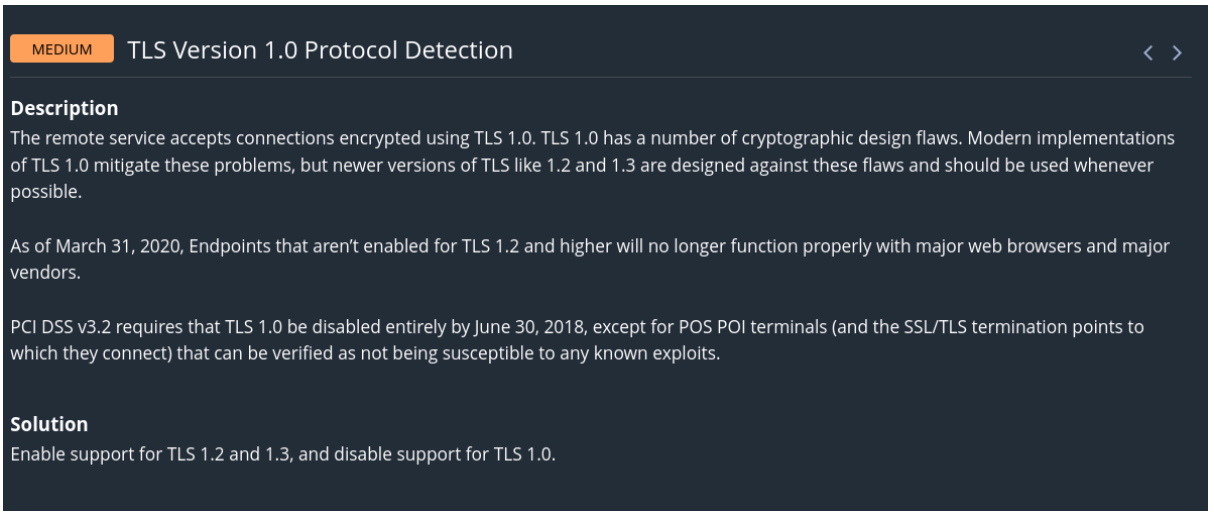
7. **CRITICITA’ 7.5 Server NFS condivisione esposta**



Descrizione
Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (basato su hostname, IP o intervallo di IP). Questo permette a chiunque di accedere alle condivisioni, aumentando il rischio di accessi non autorizzati.

Soluzione
Applica restrizioni appropriate su tutte le condivisioni NFS, limitando l'accesso solo a host o reti autorizzate.

8. **CRITICITA’ 6.5 TLS obsoleto (V 1.0)**



Descrizione

Il servizio remoto accetta connessioni crittografate utilizzando TLS 1.0, una versione obsoleta che presenta vulnerabilità progettuali nella crittografia. Sebbene le implementazioni moderne di TLS 1.0 mitigino alcuni problemi, le versioni più recenti come TLS 1.2 e 1.3 sono progettate per evitare queste falle e dovrebbero essere preferite.

Dal 31 marzo 2020, i principali browser e fornitori richiedono TLS 1.2 o superiore, rendendo TLS 1.0 incompatibile con molti servizi. Inoltre, lo standard PCI DSS v3.2 impone la disabilitazione di TLS 1.0 entro il 30 giugno 2018, ad eccezione di alcuni terminali POS/POI verificati come non vulnerabili ad exploit noti.

Soluzione
Abilita il supporto per TLS 1.2 e 1.3, e disabilita il supporto per TLS 1.0.