

SCANSIONE NESSUS METASPLOITABLE (COMMON PORTS)

Sev	CVSS	VPR	EPSS	Name	Family	Count			Host Details
CRITICAL	10.0 *			VNC Server 'pass...	Gain a shell remotely	1			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
CRITICAL	9.8	9.0	0.9737	Apache Tomcat ...	Web Servers	1			Vulnerabilities 
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			

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

Vulnerabilities 61

CRITICAL Apache Tomcat AJP Connector Request Injection (Ghostcat) < >

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

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

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.

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

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :
```

```
This produced the following truncated output (limited to 10 lines) :
```

```
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----
```

To see debug logs, please visit individual host

Port ▲

Hosts

1524 / tcp / wild_shell

192.168.50.101



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

CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL c... >

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

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

HIGH Samba Badlock Vulnerability < >

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also

<http://badlock.org>
<https://www.samba.org/samba/security/CVE-2016-2118.html>

Output

```
Nessus detected that the Samba Badlock patch has not been applied.
```

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

HIGH NFS Shares World Readable < >

Description
The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Solution
Place the appropriate restrictions on all NFS shares.

See Also
<http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>

Output

```
The following shares have no access restrictions :  
  
/ *
```

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)

MEDIUM TLS Version 1.0 Protocol Detection < >

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 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.