



Version 10.3.0-debian9\_amd64

# METASPLOITABLE

Report generated by Nessus™

Thu, 24 Nov 2022 14:55:01 EDT

---

TABLE OF CONTENTS

---

**Vulnerabilities by Host**

• 192.168.50.101 .....	4
------------------------	---

---

## **Vulnerabilities by Host**

---

192.168.50.101

10

CRITICAL

6

HIGH

23

MEDIUM

5

LOW

126

INFO

## Scan Information

Start time: Thu Aug 4 08:37:10 2022

End time: Thu Aug 4 09:03:51 2022

## Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.50.101

MAC Address: 08:00:27:52:71:A7

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

## Vulnerabilities

**134862 - Apache Tomcat A JP Connector Request Injection (Ghostcat)**

### Sinossi

È presente un connettore A JP vulnerabile in ascolto sull'host remoto.

### Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file in un connettore JP. Un utente malintenzionato remoto e non autenticato può sfruttare questa vulnerabilità per leggere i file dell'applicazione 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 remoto (RCE).

### See Also

<http://www.nessus.org/u?8ebe6246>

<http://www.nessus.org/u?4e287adb>

<http://www.nessus.org/u?cbc3d54e>

<https://access.redhat.com/security/cve/CVE-2020-1745>

<https://access.redhat.com/solutions/4851251>

<http://www.nessus.org/u?dd218234>

<http://www.nessus.org/u?dd772531>

http://www.nessus.org/u?2a01d6bf  
http://www.nessus.org/u?3b5af27e  
http://www.nessus.org/u?9dab109f  
http://www.nessus.org/u?5eafcf70

## Solution

Aggiornare una configurazione JP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o versioni successive.

Risk

FactorHigh

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

## References

CVE	CVE-2020-1745
CVE	CVE-2020-1938
XREF	CISA-KNOWN-EXPLOITED:2022/03/17

## Plugin Information

Published: 2020/03/24, Modified: 2022/07/19

## Plugin Output

tcp/8009/ajp13

Nessus was able to exploit the issue using the following request :

```
0x0000: 02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F    ....HTTP/1.1.../
0x0010: 61 73 64 66 2F 78 78 78 78 2E 6A 73 70 00 00    asdf/xxxxx.jsp..
```

```

0x0020: 09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C .localhost. ....l
0x0030: 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06 ocalhost..P.....
0x0040: 00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41 ..keep-alive...A
0x0050: 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00 ccept-Language..
0x0060: 0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00 .en-US,en;q=0.5.
0x0070: A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45 ....0...Accept-E
0x0080: 6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20 ncoding...gzip,
0x0090: 64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D deflate, sdch...
0x00A0: 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09 Cache-Control...
0x00B0: 6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F max-age=0. ...Mo
0x00C0: 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D zilla...Upgrade-
0x00D0: 49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74 Insecure-Request
0x00E0: 73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68 s...1. ...text/h
0x00F0: 74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73 tml. ...localhos
0x0100: 74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C t...!javax.servl
0x0110: 65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65 et.include.reque
0x0120: 73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61 st_uri...1... ja
0x0130: 76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C vax.servlet.incl
0x0140: 75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10 ude.path_info...
0x0150: 2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C /WEB-INF/web.xml
0x0160: 00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65 ..."javax.servle
0x0170: 74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65 t.include.servle
0x0180: 74 5F 70 61 74 68 00 00 00 00 FF t_path.....

```

This produced the following truncated output (limite [...]

## 51988 - Bind Shell Backdoor Detection

### Sinossi

L'host remoto potrebbe essere stato compromesso.

### Descrizione

Una shell è in ascolto sulla porta remota **senza** che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo connettendosi alla porta remota e inviando direttamente comandi.

### Soluzione

**Verifica se l'host remote è stato compromesso e reinstalla il Sistema se necessario.**

### Risk Factor

Critical

### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

### Plugin Output

tcp/1524/wild\_shell

```
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 .....
```

### Sinossi

Le chiavi host SSH remote sono deboli.

### Descrizione

La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto al fatto che un packager Debian rimuove 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 impostare la decifratura della sessione remota o impostare un attacco man in the middle.

### See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

### Solution

Si consideri tutto il materiale crittografico generato sull'host remoto da indovinare. In particolare, tutto il materiale chiave SSH, SSL e OpenVPN dovrebbe essere rigenerato.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

### References

BID 29179

CVE CVE-2008-0166

XREF CWE:310

Exploitable With

Core Impact (true)



## Plugin Information

Published: 2008/05/14, Modified: 2018/11/15

## Plugin Output

tcp/22/ssh

## 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

### Sinossi

Il certificato SSL remoto utilizza una chiave debole.

### Descrizione

Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto al fatto che un packager Debian rimuove 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.

### See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

### Solution

Si consideri tutto il materiale crittografico generato sull'host remoto da indovinare. In particolare, tutto il materiale chiave SSH, SSL e OpenVPN dovrebbe essere rigenerato.

### Risk Factor

### Critical

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

### References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

### Exploitable With

Core Impact (true)

## Plugin Information

---

Published: 2008/05/15, Modified: 2020/11/16

## Plugin Output

tcp/25/smtp

### Sinossi

Il certificato SSL remoto utilizza una chiave debole.

### Descrizione

Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto al fatto che un packager Debian rimuove 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.

### See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

### Solution

Si consideri tutto il materiale crittografico generato sull'host remoto da indovinare. In particolare, tutto il materiale chiave SSH, SSL e OpenVPN dovrebbe essere rigenerato.

### Risk Factor

Critical

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

### References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

### Exploitable With

Core Impact (true)

## Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

## Plugin Output

tcp/5432/postgresql

## 11356 - NFS Exported Share Information Disclosure

### Sinossi

È possibile accedere alle condivisioni NFS sull'host remoto.

### Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto può essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file su host remoto.

### Soluzione

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le condivisioni remote.

### Risk Factor

Critical

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

### Exploitable With

Metasploit (true)

### Plugin Information

Published: 2003/03/12, Modified: 2018/09/17

### Plugin Output

The following NFS shares could be mounted :

```
+ /  
+ Contents of / :  
- .  
- ..  
- bin  
- boot  
- cdrom
```

udp/2049/rpc-nfs



- dev
- etc
- home
- initrd
- initrd.img
- lib
- lost+found
- media
- mnt
- nohup.out
- opt
- proc
- root
- sbin
- srv
- sys
- tmp
- usr
- var
- vmlinuz

### Sinossi

Il servizio remoto crittografa il traffico utilizzando un protocollo con punti deboli noti.

### Descrizione

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

1. Uno schema di riempimento insicuro con cifrari CBC.
2. Schemi di rinegoziazione e ripresa delle sessioni insicuri.

Un utente malintenzionato può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i client.

Sebbene SSL / TLS abbia un mezzo sicuro per scegliere la versione più supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano nulla di meglio), molti browser Web implementano questo in modo non sicuro che consente un malintenzionato per eseguire il downgrade di una connessione (ad esempio in POODLE). Pertanto, si consiglia di disabilitare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di applicazione trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia forte" del SSC PCI.

### 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>

### Solution

Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizzare TLS 1.2 (con suite di cifratura approvate) o superiore.

Risk Factor

Critical

CVSS v3.0 Base Score

## CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

## Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

## Plugin Output

tcp/25/smtp

- SSLv2 is enabled and the server supports at least one cipher.

## Low Strength Ciphers (&lt;= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-RC2-CBC-MD5		RSA (512)	RSA	RC2-CBC (40)	MD5
export					
EXP-RC4-MD5		RSA (512)	RSA	RC4 (40)	MD5
export					

## Medium Strength Ciphers (&gt; 64-bit and &lt; 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-MD5		RSA	RSA	3DES-CBC (168)	MD5

## High Strength Ciphers (&gt;= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RC4-MD5		RSA	RSA	RC4 (128)	MD5

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

- SSLv3 is enabled and the server supports at least one cipher.

Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

## Low Strength Ciphers (&lt;= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-EDH-RSA-DES-CBC-SHA		DH (512)	RSA	DES-CBC (40)	
SHA1 export					
EDH-RSA-DES-CBC-SHA		DH	RSA	DES-CBC (56)	SHA
[...]					

### Sinossi

Il servizio remoto crittografa il traffico utilizzando un protocollo con punti deboli noti.

### Descrizione

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

1. Uno schema di riempimento insicuro con cifrari CBC.
2. Schemi di rinegoziazione e ripresa delle sessioni insicuri.

Un utente malintenzionato può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i client.

Sebbene SSL / TLS abbia un mezzo sicuro per scegliere la versione più supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano nulla di meglio), molti browser Web implementano questo in modo non sicuro che consente un malintenzionato per eseguire il downgrade di una connessione (ad esempio in POODLE). Pertanto, si consiglia di disabilitare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di applicazione trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia forte" del SSC PCI.

### 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>

### Solution

Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizzare TLS 1.2 (con suite di cifratura approvate) o superiore.

### Risk Factor

### Critical

### CVSS v3.0 Base Score

## CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

## Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

## Plugin Output

tcp/5432/postgresql

- SSLv3 is enabled and the server supports at least one cipher.  
 Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
EDH-RSA-DES-CBC3-SHA SHA1		DH	RSA	3DES-CBC (168)	
DES-CBC3-SHA SHA1		RSA	RSA	3DES-CBC (168)	

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
DHE-RSA-AES128-SHA SHA1		DH	RSA	AES-CBC (128)	
DHE-RSA-AES256-SHA SHA1		DH	RSA	AES-CBC (256)	
AES128-SHA SHA1		RSA	RSA	AES-CBC (128)	
AES256-SHA SHA1		RSA	RSA	AES-CBC (256)	
RC4-SHA SHA1		RSA	RSA	RC4 (128)	

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

## 33850 - Unix Operating System Unsupported Version Detection

### Sinossi

Il sistema operativo in esecuzione sull'host remoto non è più supportato.

### Descrizione

In base al numero di versione auto-riportato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.

La mancanza di supporto implica che nessuna nuova patch di sicurezza per il prodotto verrà rilasciata dal fornitore. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

### Solution

Eseguire l'aggiornamento a una versione del sistema operativo Unix attualmente supportata.

### Risk Factor

Critical

### CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### References

XREF IAVA:0001-A-0502

XREF IAVA:0001-A-0648

### Plugin Information

Published: 2008/08/08, Modified: 2022/05/18

### Plugin Output

tcp/0

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).  
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.
```

```
For more information, see : https://wiki.ubuntu.com/Releases
```

## 61708 - VNC Server 'password' Password

### Sinossi

Un server VNC in esecuzione sull'host remoto è protetto con una password debole.

### Descrizione

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

### Solution

Metti in sicurezza il servizio VNC con una password più efficace e complessa.

### Risk Factor

Critical

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

### Plugin Output

tcp/5900/vnc

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

### Sinossi

Il server dei nomi remoto è interessato da una vulnerabilità legata a un errore di asserzione.

### Descrizione

Esiste una vulnerabilità ad attacchi di tipo Denial of Service (DoS) nelle versioni di ISC BIND 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 e versioni precedenti. Un utente malintenzionato remoto non autenticato può sfruttare questo problema, tramite un messaggio appositamente predisposto, per impedire al servizio di rispondere.

Si noti che Nessus non ha verificato questo problema, ma ha invece fatto affidamento solo sul numero di versione auto-segnalato dell'applicazione.

### See Also

<https://kb.isc.org/docs/cve-2020-8617>

### Solution

Aggiornamento alla versione aggiornata strettamente correlata alla versione corrente di BIND.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

### CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

### STIG Severity

I

### References



CVE CVE-2020-8617  
XREF IAVA:2020-A-0217-S

#### Plugin Information

---

Published: 2020/05/22, Modified: 2022/05/13

#### Plugin Output

udp/53/dns

```
Installed version : 9.4.2  
Fixed version    : 9.11.19
```

### Sinossi

Il server dei nomi remoto è interessato dalle vulnerabilità di Service Downgrade/Reflected DoS.

### Descrizione

In base alla versione auto-rapportata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è interessata dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Ciò è dovuto al fatto che BIND DNS non limita sufficientemente il numero di recuperi che possono essere eseguiti durante l'elaborazione di una risposta di riferimento.

Un utente malintenzionato remoto non autenticato può sfruttare questo problema per causare una riduzione del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione.

### See Also

<https://kb.isc.org/docs/cve-2020-8616>

### Solution

Aggiornamento della versione BIND di ISC a cui si fa riferimento nella consulenza del fornitore.

### Risk Factor

Medium

### CVSS v3.0 Base Score

8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

### CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### STIG Severity

I

### References

CVE CVE-2020-8616  
XREF IAVA:2020-A-0217-S

#### Plugin Information

---

Published: 2020/05/22, Modified: 2020/06/26

#### Plugin Output

udp/53/dns

```
Installed version : 9.4.2  
Fixed version    : 9.11.19
```

### Sinossi

Il server NFS remoto esporta condivisioni leggibili in tutto il mondo.

### Descrizione

Il server NFS remoto esporta una o più condivisioni senza limitare l'accesso (in base al nome host, all'IP o all'intervallo IP).

### See Also

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

### Solution

Porre le opportune restrizioni su tutte le azioni NFS.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2009/10/26, Modified: 2020/05/05

### Plugin Output

tcp/2049/rpc-nfs

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

### Sinossi

Il servizio remoto supporta l'uso di cifrari SSL di media potenza.

### Descrizione

L'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di media potenza. Nessus considera media resistenza qualsiasi crittografia che utilizza lunghezze di chiave di almeno 64 bit e meno di 112 bit, oppure che utilizza la suite di crittografia 3DES.

Si noti che è notevolmente più facile aggirare la crittografia di media potenza se l'utente malintenzionato si trova sulla stessa rete fisica.

### See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>

<https://sweet32.info>

### Solution

Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrari a media resistenza.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### References

CVE CVE-2016-2183

### Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

### Plugin Output

tcp/25/smtp

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-MD5	0x07, 0x00, 0xC0	RSA	RSA	3DES-CBC (168)	MD5
EDH-RSA-DES-CBC3-SHA	0x00, 0x16	DH	RSA	3DES-CBC (168)	
SHA1					
ADH-DES-CBC3-SHA	0x00, 0x1B	DH	None	3DES-CBC (168)	
SHA1					
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	
SHA1					

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

### Sinossi

Il servizio remoto supporta l'uso di cifrari SSL di media potenza.

### Descrizione

L'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di media potenza. Nessus considera media resistenza qualsiasi crittografia che utilizza lunghezze di chiave di almeno 64 bit e meno di 112 bit, oppure che utilizza la suite di crittografia 3DES.

Si noti che è notevolmente più facile aggirare la crittografia di media potenza se l'utente malintenzionato si trova sulla stessa rete fisica.

### See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>

<https://sweet32.info>

### Solution

Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrari a media resistenza.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### References

CVE CVE-2016-2183

### Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

### Plugin Output

tcp/5432/postgresql

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
EDH-RSA-DES-CBC3-SHA	0x00, 0x16	DH	RSA	3DES-CBC (168)	
SHA1					
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	
SHA1					

The fields above are :

{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}



### Sinossi

Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.

### Descrizione

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, che esiste nel Security Account Manager (SAM) e Local Autorità di sicurezza (Criterio del dominio) (LSAD) a causa di una negoziazione errata del livello di autenticazione sui canali RPC (Remote Procedure Call). Un malintenzionato man-in-the-middle che è in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questo difetto per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, ad esempio la visualizzazione o la modifica di dati di protezione sensibili nel database di Active Directory (AD) o la disabilitazione dei servizi critici.

### See Also

<http://badlock.org>

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

### Solution

Aggiornamento alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 orù successive.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

### CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

BID 86002

CVE CVE-2016-2118  
XREF CERT:813296

#### Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

#### Plugin Output

tcp/445/cifs

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

### Sinossi

Le funzioni di debug sono abilitate sul server Web remoto.

### Descrizione

Il server Web remoto supporta i metodi TRACE e/o TRACK. TRACE e TRACK sono metodi HTTP utilizzati per eseguire il debug delle connessioni al server Web.

### See Also

[https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper\\_XST\\_ebook.pdf](https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf)

<http://www.apacheweek.com/issues/03-01-24>

<https://download.oracle.com/sunalerts/1000718.1.html>

### Solution

Disable these HTTP methods. Refer to the plugin output for more information.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

BID	9506
BID	9561
BID	11604
BID	33374

BID 37995  
CVE CVE-2003-1567  
CVE CVE-2004-2320  
CVE CVE-2010-0386  
XREF CERT:288308  
XREF CERT:867593  
XREF CWE:16  
XREF CWE:200

## Plugin Information

Published: 2003/01/23, Modified: 2020/06/12

## Plugin Output

tcp/80/www

To disable these methods, add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

Nessus sent the following TRACE request :

```
..... snip .....
TRACE /Nessus2114587619.html HTTP/1.1
Connection: Close
Host: 192.168.50.101
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

..... snip .....  
and received the following response from the remote server :

```
..... snip .....
HTTP/1.1 200 OK
Date: Thu, 04 Aug 2022 12:45:02 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE /Nessus2114587619.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.50.101
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

Accept-Language: en  
Accept-Charset: iso-8859-1,\*,utf-8

..... snip .....

## Sinossi

Il server dei nomi **remoto** è interessato da una vulnerabilità ad attacchi di tipo Denial of Service.

## Descrizione

In base al numero di versione auto-riportato, l'installazione di ISC BIND in esecuzione sul server **dei nomi remoto** è la versione 9.x precedente alla 9.11.22, 9.12.x precedente alla 9.16.6 o 9.17.x precedente alla 9.17.4. È pertanto interessato da una vulnerabilità ad attacchi di tipo Denial of Service (DoS) dovuta a un errore di asserzione durante il tentativo di verificare una risposta troncata a una **richiesta** firmata TSIG. Un utente malintenzionato remoto autenticato può sfruttare questo problema inviando **una** risposta troncata a una richiesta firmata TSIG per attivare un **errore** di asserzione, causando la chiusura del server.

Si noti che Nessus non ha verificato questo problema, ma ha invece fatto affidamento solo sul numero di versione auto-segnalato dell'applicazione.

## See Also

<https://kb.isc.org/docs/cve-2020-8622>

## Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

## CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

## CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

## CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

## STIG Severity

I

## References

---

CVE	CVE-2020-8622
XREF	IAVA:2020-A-0385-S

## Plugin Information

---

Published: 2020/08/27, Modified: 2021/06/03

## Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version    : 9.11.22, 9.16.6, 9.17.4 or later
```

## Sinossi

La firma non è richiesta sul server SMB remoto.

## Descrizione

La firma non è richiesta sul server SMB remoto. Un utente malintenzionato remoto non autenticato può sfruttare questo problema per condurre attacchi man-in-the-middle contro il server SMB.

## See Also

<http://www.nessus.org/u?df39b8b3>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

<http://www.nessus.org/u?a3cac4ea>

## Soluzione

Applicare la firma dei messaggi nella configurazione dell'host. In Windows, si trova nell'impostazione dei criteri "Server di rete Microsoft: comunicazioni con firma digitale (sempre)". Su Samba, l'impostazione è chiamata "firma del server". Vedi i link "vedi anche" per ulteriori dettagli.

## Risk Factor

Medium

## CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

## CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

## CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

## CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

## Plugin Information



Published: 2012/01/19, Modified: 2021/03/15

Plugin Output

tcp/445/cifs

### Sinossi

Il servizio di posta remota consente l'inserimento di comandi in chiaro durante la negoziazione di un canale di comunicazione crittografato.

### Descrizione

Il servizio SMTP remoto contiene un difetto software nell'implementazione STARTTLS che potrebbe consentire a un utente malintenzionato remoto e non autenticato di inserire comandi durante la fase di protocollo in testo normale che verranno eseguiti durante la fase di protocollo con testo crittografato.

Uno sfruttamento riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o le credenziali SASL (Simple Authentication and Security Layer) associate.

### See Also

<https://tools.ietf.org/html/rfc2487>

<https://www.securityfocus.com/archive/1/516901/30/0/threaded>

### Soluzione

Contattare il fornitore per verificare se è disponibile un aggiornamento.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

### CVSS v2.0 Temporal Score

3.1 (CVSS2#E:POC/RL:OF/RC:C)

### References

BID	46767
CVE	CVE-2011-0411
CVE	CVE-2011-1430
CVE	CVE-2011-1431
CVE	CVE-2011-1432
CVE	CVE-2011-1506
CVE	CVE-2011-2165
XREF	CERT:555316

## Plugin Information

---

Published: 2011/03/10, Modified: 2019/03/06

## Plugin Output

tcp/25/smtp

```
Nessus sent the following two commands in a single packet :
```

```
STARTTLS\r\nRSET\r\n
```

```
And the server sent the following two responses :
```

```
220 2.0.0 Ready to start TLS
```

```
250 2.0.0 Ok
```

### Sinossi

Il server SSH remoto è configurato per consentire algoritmi di crittografia deboli o nessun algoritmo .

### Descrizione

Nessus ha rilevato che il server SSH remoto è configurato per utilizzare il cifrario a flusso Arcfour o nessun cifrario . RFC 4253 sconsiglia l'utilizzo di Arcfour a causa di un problema con i tasti deboli.

### See Also

<https://tools.ietf.org/html/rfc4253#section-6.3>

### Soluzione

Contattare il fornitore o consultare la documentazione del prodotto per rimuovere i codici deboli.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

### Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :
```

```
arcfour
arcfour128
arcfour256
```

```
The following weak client-to-server encryption algorithms are supported :
```

```
arcfour
arcfour128
arcfour256
```

### Sinossi

Il servizio remoto supporta l'utilizzo di cifrari SSL anonimi.

### Descrizione

L'host remoto supporta l'utilizzo di crittografia SSL anonimi. Sebbene ciò consenta a un amministratore di configurare un servizio che crittografa il traffico senza dover generare e configurare certificati SSL, non offre alcun modo per verificare l'identità dell'host remoto e rende il servizio vulnerabile a un **attacco** man-in-the-middle.

Nota: questo è notevolmente più facile da sfruttare se l'utente malintenzionato si trova sulla stessa rete fisica.

### See Also

<http://www.nessus.org/u?3a040ada>

### Soluzione

Riconfigurare l'applicazione interessata, se possibile, per evitare l'utilizzo di codici deboli.

### Risk Factor

Low

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

### References

BID 28482

CVE CVE-2007-1858

### Plugin Information

## Plugin Output

tcp/25/smtp

The following is a list of SSL anonymous ciphers supported by the remote TCP server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-ADH-DES-CBC-SHA SHA1 export	0x00, 0x19	DH (512)	None	DES-CBC (40)	
EXP-ADH-RC4-MD5 export	0x00, 0x17	DH (512)	None	RC4 (40)	MD5
ADH-DES-CBC-SHA SHA1	0x00, 0x1A	DH	None	DES-CBC (56)	

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
ADH-DES-CBC3-SHA SHA1	0x00, 0x1B	DH	None	3DES-CBC (168)	

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
ADH-AES128-SHA SHA1	0x00, 0x34	DH	None	AES-CBC (128)	
ADH-AES256-SHA SHA1	0x00, 0x3A	DH	None	AES-CBC (256)	
ADH-RC4-MD5	0x00, 0x18	DH	None	RC4 (128)	MD5

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

### Sinossi

Il certificato SSL per questo servizio non può essere considerato attendibile.

### Descrizione

Il certificato X.509 del server non può essere considerato attendibile. Questa situazione può verificarsi in tre modi diversi, in cui la catena di fiducia può essere interrotta, come indicato di seguito :

1. Innanzitutto, la parte superiore della catena di certificati inviata dal server potrebbe non discendere da un'autorità di certificazione pubblica nota. Ciò può verificarsi quando la **parte superiore della catena è un certificato autofirmato non riconosciuto** o quando mancano **certificati** intermedi che collegherebbero la parte superiore della catena di certificati a un'autorità di certificazione pubblica nota.
2. In secondo luogo , la catena di certificati può contenere un certificato non valido al momento dell'analisi. Ciò può verificarsi quando l'analisi viene eseguita prima di una delle date "notBefore" del certificato o dopo una delle date "notAfter" del certificato .
3. **In terzo luogo**, la catena di certificati può contenere una firma **che non** corrisponde alle informazioni del certificato e **o** che non è stato possibile verificare. Le firme errate possono essere corrette ottenendo che il certificato con la firma errata venga nuovamente firmato dall'autorità emittente. Le firme che non è stato possibile verificare sono il risultato dell'emittente del certificato che utilizza un algoritmo di firma che Nessus **non** supporta o non riconosce.

Se l'host remoto è un host pubblico in produzione, qualsiasi interruzione nella catena rende più difficile per gli utenti verificare l'autenticità e l'identità del server Web. Ciò potrebbe semplificare l'esecuzione di attacchi man-in-the-middle contro l'host remoto.

### See Also

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

### Soluzione

**Acquista o genera un certificato SSL appropriato per questo servizio.**

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

---

## Plugin Output

tcp/25/smtp

```
The following certificate was part of the certificate chain  
sent by the remote host, but it has expired :
```

```
|-Subject   : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-  
base.localdomain  
|-Not After : Apr 16 14:07:45 2010 GMT
```

```
The following certificate was at the top of the certificate  
chain sent by the remote host, but it is signed by an unknown  
certificate authority :
```

```
|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-  
base.localdomain  
|-Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-  
base.localdomain
```



### Sinossi

Il certificato SSL per questo servizio non può essere considerato attendibile.

### Descrizione

Il certificato X.509 del server non può essere considerato attendibile. Questa situazione può verificarsi in tre modi diversi, in cui la catena di fiducia può essere interrotta, come indicato di seguito :

1. Innanzitutto, la parte superiore della catena di certificati inviata dal server potrebbe non discendere da un'autorità di certificazione pubblica nota. Ciò può verificarsi quando la **parte superiore della catena è un certificato autofirmato non riconosciuto** o quando mancano **certificati** intermedi che collegherebbero la parte superiore della catena di certificati a un'autorità di certificazione pubblica nota.
2. In secondo luogo , la catena di certificati può contenere un certificato non valido al momento dell'analisi. Ciò può verificarsi quando l'analisi viene eseguita prima di una delle date "notBefore" del certificato o dopo una delle date "notAfter" del certificato .
3. In terzo luogo, la catena di certificati può contenere una firma che non corrisponde alle informazioni del certificato o che non può essere verificata. Le firme errate possono essere corrette ottenendo **che il certificato con la firma errata venga nuovamente firmato dall'autorità emittente**. Le firme **che non** è stato possibile verificare sono il risultato dell'emittente del certificato **che** utilizza un algoritmo di firma che Nessus **non** supporta o non riconosce.

Se l'host remoto è un host pubblico in produzione, qualsiasi interruzione nella catena rende più difficile per gli utenti verificare l'autenticità e l'identità del server Web. Ciò potrebbe semplificare l'esecuzione di attacchi man-in-the-middle contro l'host remoto.

### See Also

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

### Soluzione

**Acquista o genera un certificato SSL appropriato per questo servizio.**

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

## Plugin Output

tcp/5432/postgresql

The following certificate was part of the certificate chain sent by the remote host, but it has expired :

```
| -Subject    : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
| -Not After  : Apr 16 14:07:45 2010 GMT
```

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

```
| -Subject    : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
| -Issuer     : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

## 15901 - SSL Certificate Expiry

### Sinossi

Il certificato SSL del server remoto è già scaduto.

### Descrizione

Questo plugin controlla le date di scadenza dei certificati associati ai servizi abilitati SSL sulla destinazione e segnala se alcuni sono già scaduti.

### Soluzione

Acquista o genera un nuovo certificato SSL per sostituire quello esistente.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

### Plugin Output

tcp/25/smtp

The SSL certificate has already expired :

```
Subject      : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
emailAddress=root@ubuntu804-base.localdomain
Issuer       : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
emailAddress=root@ubuntu804-base.localdomain
Not valid before : Mar 17 14:07:45 2010 GMT
Not valid after  : Apr 16 14:07:45 2010 GMT
```

## 15901 - SSL Certificate Expiry

### Sinossi

Il certificato SSL del server remoto è già scaduto.

### Descrizione

Questo plugin controlla le date di scadenza dei certificati associati ai servizi abilitati SSL sulla destinazione e segnala se alcuni sono già scaduti.

### Soluzione

Acquista o genera un nuovo certificato SSL per sostituire quello esistente.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

### Plugin Output

tcp/5432/postgresql

The SSL certificate has already expired :

```
Subject      : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
emailAddress=root@ubuntu804-base.localdomain
Issuer       : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
emailAddress=root@ubuntu804-base.localdomain
Not valid before : Mar 17 14:07:45 2010 GMT
Not valid after  : Apr 16 14:07:45 2010 GMT
```

## 45411 - SSL Certificate with Wrong Hostname

### Sinossi

Il certificato SSL per questo servizio è per un host diverso.

### Descrizione

L'attributo 'commonName' (CN) del certificato SSL presentato per questo servizio è per un computer diverso.

### Soluzione

Acquista o genera un certificato SSL appropriato per questo servizio.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

### Plugin Output

tcp/25/smtp

```
The identities known by Nessus are :  
  
192.168.50.101  
192.168.50.101  
  
The Common Name in the certificate is :  
  
ubuntu804-base.localdomain
```

## 45411 - SSL Certificate with Wrong Hostname

### Sinossi

Il certificato SSL per questo servizio è per un host diverso.

### Descrizione

L'attributo 'commonName' (CN) del certificato SSL presentato per questo servizio è per un computer diverso.

### Soluzione

Acquista o genera un certificato SSL appropriato per questo servizio.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

### Plugin Output

tcp/5432/postgresql

```
The identities known by Nessus are :
```

```
192.168.50.101
192.168.50.101
```

```
The Common Name in the certificate is :
```

```
ubuntu804-base.localdomain
```

## 89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

### Sinossi

L'host remoto può essere interessato da una vulnerabilità che consente a un utente malintenzionato remoto di decrittografare potenzialmente il traffico TLS acquisito.

### Descrizione

L'host remoto supporta SSLv2 e pertanto può essere interessato da una vulnerabilità che consente un attacco oracolo di padding di Bleichenbacher cross-protocol noto come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Questa vulnerabilità esiste a causa di un difetto nell'implementazione di Secure Sockets Layer Version 2 (SSLv2) e consente di decrittografare il traffico TLS acquisito. Un utente malintenzionato man-in-the-middle può sfruttare questo per decrittografare la connessione TLS utilizzando il traffico precedentemente acquisito e la crittografia debole insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata.

### See Also

<https://drownattack.com/>

<https://drownattack.com/drown-attack-paper.pdf>

### Soluzione

Disabilitare SSLv2 ed esportare suite di crittografia crittografica. Assicurarsi che le chiavi private non vengano utilizzate ovunque con software server che supporta connessioni SSLv2.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

### References

BID 83733  
CVE CVE-2016-0800  
XREF CERT:583776

## Plugin Information

Published: 2016/03/01, Modified: 2019/11/20

## Plugin Output

tcp/25/smtp

The remote host is affected by SSL DROWN and supports the following vulnerable cipher suites :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-RC2-CBC-MD5 export	0x04, 0x00, 0x80	RSA (512)	RSA	RC2-CBC (40)	MD5
EXP-RC4-MD5 export	0x02, 0x00, 0x80	RSA (512)	RSA	RC4 (40)	MD5

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RC4-MD5	0x01, 0x00, 0x80	RSA	RSA	RC4 (128)	MD5

The fields above are :

{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}



### Sinossi

Il servizio remoto supporta l'uso del codice RC4.

### Descrizione

L'host remoto supporta l'uso di RC4 in una o più suite di cifratura.

Il cifrario RC4 è difettoso nella sua generazione di un flusso pseudo-casuale di byte in modo che un'ampia varietà di piccoli pregiudizi vengano introdotti nel flusso, diminuendo la sua casualità.

Se il testo non crittografato viene ripetutamente crittografato (ad esempio, cookie HTTP) e un utente malintenzionato è in grado di ottenere molti (cioè decine di milioni) testi cifrati, l'utente malintenzionato potrebbe essere in grado di derivare il testo in chiaro.

### See Also

<https://www.rc4nomore.com/>

<http://www.nessus.org/u?ac7327a0>

<http://cr.yip.to/talks/2013.03.12/slides.pdf>

<http://www.isg.rhul.ac.uk/tls/>

[https://www.imperva.com/docs/HII\\_Attacking\\_SSL\\_when\\_using\\_RC4.pdf](https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf)

### Soluzione

Riconfigurare l'applicazione interessata, se possibile, per evitare l'utilizzo di crittografie RC4. Prendi in considerazione l'utilizzo di TLS 1.2 con suite AES-GCM soggette al supporto di browser e server Web.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

## References

BID 58796  
BID 73684  
CVE CVE-2013-2566  
CVE CVE-2015-2808

## Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

## Plugin Output

tcp/25/smtp

List of RC4 cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-RC4-MD5 export	0x02, 0x00, 0x80	RSA (512)	RSA	RC4 (40)	MD5
EXP-ADH-RC4-MD5 export	0x00, 0x17	DH (512)	None	RC4 (40)	MD5
EXP-RC4-MD5 export	0x00, 0x03	RSA (512)	RSA	RC4 (40)	MD5

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RC4-MD5	0x01, 0x00, 0x80	RSA	RSA	RC4 (128)	MD5
ADH-RC4-MD5	0x00, 0x18	DH	None	RC4 (128)	MD5
RC4-MD5	0x00, 0x04	RSA	RSA	RC4 (128)	MD5
RC4-SHA	0x00, 0x05	RSA	RSA	RC4 (128)	MD5

SHA1

The fields above are :

{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}

### Sinossi

Il servizio remoto supporta l'uso del codice RC4.

### Descrizione

L'host remoto supporta l'uso di RC4 in una o più suite di cifratura.

Il cifrario RC4 è difettoso nella sua generazione di un flusso pseudo-casuale di byte in modo che un'ampia varietà di piccoli pregiudizi vengano introdotti nel flusso, diminuendo la sua casualità.

Se il testo non crittografato viene ripetutamente crittografato (ad esempio, cookie HTTP) e un utente malintenzionato è in grado di ottenere molti (cioè decine di milioni) testi cifrati, l'utente malintenzionato potrebbe essere in grado di derivare il testo in chiaro.

### See Also

<https://www.rc4nomore.com/>

<http://www.nessus.org/u?ac7327a0>

<http://cr.yp.to/talks/2013.03.12/slides.pdf>

<http://www.isg.rhul.ac.uk/tls/>

[https://www.imperva.com/docs/HII\\_Attacking\\_SSL\\_when\\_using\\_RC4.pdf](https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf)

### Soluzione

Riconfigurare l'applicazione interessata, se possibile, per evitare l'utilizzo di crittografie RC4. Prendi in considerazione l'utilizzo di TLS 1.2 con suite AES-GCM soggette al supporto di browser e server Web.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

## References

BID 58796  
BID 73684  
CVE CVE-2013-2566  
CVE CVE-2015-2808

## Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

## Plugin Output

tcp/5432/postgresql

List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RC4-SHA	0x00, 0x05	RSA	RSA	RC4(128)	
SHA1					

The fields above are :

{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}

### Sinossi

La catena di certificati SSL per questo servizio termina con un certificato autofirmato non riconosciuto.

### Descrizione

La catena di certificati X.509 per questo servizio non è firmata da un'autorità di certificazione riconosciuta. Se l'host remoto è un host pubblico in produzione, ciò annulla l'uso di SSL in quanto chiunque potrebbe stabilire un attacco man-in-the-middle contro l'host remoto.

Si noti che questo plugin non controlla le catene di certificati che terminano con un certificato che non è autofirmato, ma è firmato da un'autorità di certificazione non riconosciuta.

### Soluzione

Acquista o genera un certificato SSL appropriato per questo servizio.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

### Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

### Plugin Output

tcp/25/smtp

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :
```

```
|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

### Sinossi

La catena di certificati SSL per questo servizio termina con un certificato autofirmato non riconosciuto.

### Descrizione

La catena di certificati X.509 per questo servizio non è firmata da un'autorità di certificazione riconosciuta. Se l'host remoto è un host pubblico in produzione, ciò annulla l'uso di SSL in quanto chiunque potrebbe stabilire un attacco man-in-the-middle contro l'host remoto.

Si noti che questo plugin non controlla le catene di certificati che terminano con un certificato che non è autofirmato, ma è firmato da un'autorità di certificazione non riconosciuta.

### Soluzione

Acquista o genera un certificato SSL appropriato per questo servizio.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

### Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

### Plugin Output

tcp/5432/postgresql

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :
```

```
|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

## 26928 - SSL Weak Cipher Suites Supported

### Sinossi

Il servizio remoto supporta l'utilizzo di codici SSL deboli.

### Descrizione

L'host remoto supporta l'utilizzo di crittografia SSL che offrono una crittografia debole .

Nota: questo è notevolmente più facile da sfruttare se l'utente malintenzionato si trova sulla stessa rete fisica.

### See Also

<http://www.nessus.org/u?6527892d>

### Soluzione

Riconfigurare l'applicazione interessata, se possibile per evitare l'utilizzo di codici deboli.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

### Plugin Information

Published: 2007/10/08, Modified: 2021/02/03

### Plugin Output

Here is the list of weak SSL ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-RC2-CBC-MD5 export	0x04, 0x00, 0x80	RSA (512)	RSA	RC2-CBC (40)	MD5
EXP-RC4-MD5 export	0x02, 0x00, 0x80	RSA (512)	RSA	RC4 (40)	MD5
EXP-EDH-RSA-DES-CBC-SHA SHA1 export	0x00, 0x14	DH (512)	RSA	DES-CBC (40)	
EDH-RSA-DES-CBC-SHA SHA1	0x00, 0x15	DH	RSA	DES-CBC (56)	
EXP-ADH-DES-CBC-SHA SHA1 export	0x00, 0x19	DH (512)	None	DES-CBC (40)	
EXP-ADH-RC4-MD5 export	0x00, 0x17	DH (512)	None	RC4 (40)	MD5
ADH-DES-CBC-SHA SHA1	0x00, 0x1A	DH	None	DES-CBC (56)	
EXP-DES-CBC-SHA SHA1 export	0x00, 0x08	RSA (512)	RSA	DES-CBC (40)	
EXP-RC2-CBC-MD5 export	0x00, 0x06	RSA (512)	RSA	RC2-CBC (40)	MD5
EXP-RC4-MD5 export	0x00, 0x03	RSA (512)	RSA	RC4 (40)	MD5
DES-CBC-SHA SHA1	0x00, 0x09	RSA	RSA	DES-CBC (56)	

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```



## 81606 - SSL/TLS EXPORT\_RSA <= 512-bit Cipher Suites Supported (FREAK)

### Sinossi

---

L'host remoto supporta un set di codici deboli.

### Descrizione

---

L'host remoto supporta EXPORT\_RSA suite di crittografia con chiavi inferiori o uguali a 512 bit. Un utente malintenzionato può fattorizzare un modulo RSA a 512 bit in un breve lasso di tempo.

Un utente malintenzionato man-in-the middle potrebbe essere in grado di eseguire il downgrade della sessione per utilizzare EXPORT\_RSA suite di crittografia (ad esempio CVE-2015-0204). Pertanto, si consiglia di rimuovere il supporto per le suite di crittografia deboli.

### See Also

<https://www.smacktls.com/#freak>

<https://www.openssl.org/news/secadv/20150108.txt>

<http://www.nessus.org/u?b78da2c4>

### Soluzione

---

Riconfigurare il servizio per rimuovere il supporto per EXPORT\_RSA suite di crittografia.

### Risk Factor

Medium

### CVSS v2.0 Base Score

---

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

---

3.2 (CVSS2#E:U/RL:OF/RC:C)

### References

BID	71936
CVE	CVE-2015-0204
XREF	CERT:243585

### Plugin Information

Published: 2015/03/04, Modified: 2021/02/03

### Plugin Output

---

EXPORT\_RSA cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EXP-DES-CBC-SHA SHA1 export	0x00, 0x08	RSA (512)	RSA	DES-CBC (40)	
EXP-RC2-CBC-MD5 export	0x00, 0x06	RSA (512)	RSA	RC2-CBC (40)	MD5
EXP-RC4-MD5 export	0x00, 0x03	RSA (512)	RSA	RC4 (40)	MD5

The fields above are :

- {Tenable ciphername}
- {Cipher ID code}
- Kex={key exchange}
- Auth={authentication}
- Encrypt={symmetric encryption method}
- MAC={message authentication code}
- {export flag}

### Sinossi

È possibile ottenere informazioni sensibili dall'host remoto con servizi abilitati SSL/TLS.

### Descrizione

L'host remoto è interessato da una vulnerabilità di divulgazione di informazioni personali man-in-the-middle (MitM) nota come POODLE. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di riempimento durante la decrittografia dei messaggi crittografati utilizzando cifrari a blocchi in modalità CBC (Cipher Block Chaining).

Gli aggressori MitM possono decrittografare un byte selezionato di un testo cifrato in soli 256 tentativi se sono in grado di forzare un'applicazione vittima a inviare ripetutamente gli stessi dati sulle connessioni SSL 3.0 appena create.

Finché un client e un servizio supportano entrambi SSLv3, è possibile eseguire il rollback di una connessione a SSLv3, anche se TLSv1 o versione successiva è supportata dal client e dal servizio.

Il meccanismo TLS Fallback SCSV previene gli attacchi di "version rollback" senza influire sui client legacy; Tuttavia, può proteggere le connessioni solo quando il client e il servizio supportano il meccanismo. I siti che non possono disabilitare SSLv3 immediatamente devono abilitare questo meccanismo.

Si tratta di una vulnerabilità nella specifica SSLv3, non in una particolare implementazione SSL. La disattivazione di SSLv3 è l'unico modo per attenuare completamente la vulnerabilità.

### See Also

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00>

### Solution

Disabilitare

SSLv3.

I servizi che devono supportare SSLv3 devono abilitare il meccanismo SCSV di fallback TLS fino a quando SSLv3 non può essere disabilitato.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

## CVSS v2.0 Base Score

---

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

## CVSS v2.0 Temporal Score

---

3.2 (CVSS2#E:U/RL:OF/RC:C)

## References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

## Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

## Plugin Output

tcp/25/smtp

Nessus determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.

### Sinossi

È possibile ottenere informazioni sensibili dall'host remoto con servizi abilitati SSL/TLS.

### Descrizione

L'host remoto è interessato da una vulnerabilità di divulgazione di informazioni personali man-in-the-middle (MitM) nota come POODLE. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di riempimento durante la decrittografia dei messaggi crittografati utilizzando cifrari a blocchi in modalità CBC (Cipher Block Chaining).

Gli aggressori MitM possono decrittografare un byte selezionato di un testo cifrato in soli 256 tentativi se sono in grado di forzare un'applicazione vittima a inviare ripetutamente gli stessi dati sulle connessioni SSL 3.0 appena create.

Finché un client e un servizio supportano entrambi SSLv3, è possibile eseguire il rollback di una connessione a SSLv3, anche se TLSv1 o versione successiva è supportata dal client e dal servizio.

Il meccanismo TLS Fallback SCSV previene gli attacchi di "version rollback" senza influire sui client legacy; Tuttavia, può proteggere le connessioni solo quando il client e il servizio supportano il meccanismo. I siti che non possono disabilitare SSLv3 immediatamente devono abilitare questo meccanismo.

Si tratta di una vulnerabilità nella specifica SSLv3, non in una particolare implementazione SSL. La disattivazione di SSLv3 è l'unico modo per attenuare completamente la vulnerabilità.

### See Also

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00>

### Soluzione

#### Disabilitare

#### SSLv3.

I servizi che devono supportare SSLv3 devono abilitare il meccanismo SCSV di fallback TLS fino a quando SSLv3 non può essere disabilitato.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

## CVSS v2.0 Base Score

---

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

## CVSS v2.0 Temporal Score

---

3.2 (CVSS2#E:U/RL:OF/RC:C)

## References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

## Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

## Plugin Output

tcp/5432/postgresql

Nessus determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.

### Sinossi

Il servizio remoto crittografa il traffico utilizzando una versione precedente di TLS.

### Descrizione

Il servizio remoto accetta connessioni crittografate tramite TLS 1.0. TLS 1.0 presenta una serie di difetti di progettazione crittografica. Le moderne implementazioni di TLS 1.0 mitigano questi problemi, ma le versioni più recenti di TLS come

1.2 e 1.3 sono progettati contro questi difetti e dovrebbero essere utilizzati ogni volta che è possibile.

A partire dal 31 marzo 2020, gli endpoint non abilitati per TLS 1.2 e versioni successive non funzioneranno più correttamente con i principali browser Web e i principali fornitori.

PCI DSS v3.2 richiede che TLS 1.0 sia disabilitato completamente entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e dei punti di terminazione SSL / TLS a cui si connettono) che possono essere verificati come non suscettibili ad alcun exploit noto.

### See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

### Soluzione

Abilitare il supporto per TLS 1.2 e 1.3 e disabilitare il supporto per TLS 1.0.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

### CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

### Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

### Plugin Output

tcp/25/smtp

```
TLSv1 is enabled and the server supports at least one cipher.
```

### Sinossi

Il servizio remoto crittografa il traffico utilizzando una versione precedente di TLS.

### Descrizione

Il servizio remoto accetta connessioni crittografate tramite TLS 1.0. TLS 1.0 presenta una serie di difetti di progettazione crittografica. Le moderne implementazioni di TLS 1.0 mitigano questi problemi, ma le versioni più recenti di TLS come

1.2 e 1.3 sono progettati contro questi difetti e dovrebbero essere utilizzati ogni volta che è possibile.

A partire dal 31 marzo 2020, gli endpoint non abilitati per TLS 1.2 e versioni successive non funzioneranno più correttamente con i principali browser Web e i principali fornitori.

PCI DSS v3.2 richiede che TLS 1.0 sia disabilitato completamente entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e dei punti di terminazione SSL / TLS a cui si connettono) che possono essere verificati come non suscettibili di exploit noti.

### See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

### Soluzione

Abilitare il supporto per TLS 1.2 e 1.3 e disabilitare il supporto per TLS 1.0.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

### CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

### Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

### Plugin Output

tcp/5432/postgresql

```
TLSv1 is enabled and the server supports at least one cipher.
```



