Greenbone Security Assistant

Logged in as User **LabGroup68** | Logout

Tue Feb 20 13:56:46 2018 UTC

Scan Management **Asset Management** **SecInfo Management** **Configuration** **Extras**

Administration **Help**

Report Summary

√Apply overrides

Task

Result of Task: basic services - rome.secnet

Order of results: by host

Scan started: Tue Feb 20 13:42:54 2018

Scan ended: Tue Feb 20 13:56:42 2018

Scan status: Done

	High	Medium	Low	Log	False Pos.	Total	Run Alert	Download
Full report:	3	3	1	60	0	67		PDF
All filtered results:	3	3	0	0	0	6		PDF
Filtered results 1 - 6:	3	3	0	0	0	6		PDF

Result Filtering

Sorting: port ascending | port descending | threat ascending | threat descending

Results per page: 100

Auto-FP:

- [ ] Trust vendor security updates
  - (•) Full CVE match
  - ( ) Partial CVE match
- [ ] Show closed CVEs

- [x] Show notes
- [x] Only show hosts that have results
- [ ] CVSS >= 8.0

Text phrase:

Threat: High Medium Low Log False Pos. Apply

Filter: --

sort-reverse=type result_hosts_only=1 min_cvss_base= levels=hm autofp=

Filtered Results 1 - 6 of 6

Host	OS	Start	End	High	Medium	Low	Log	False Pos.	Total
192.168.1.10 (rome.secnet)	?	Feb 20, 13:43:00	Feb 20, 13:56:41	3	3	0	0	0	6
Total: 1				3	3	0	0	0	6

Port summary for 192.168.1.10

Service (Port)	Threat
http-alt (8080/tcp)	High
imap (143/tcp)	High
pop3 (110/tcp)	High
general/tcp	Medium
imaps (993/tcp)	Medium
pop3s (995/tcp)	Medium

Security Issues reported for 192.168.1.10

High (CVSS: 6.8) http-alt (8080/tcp)
NVT: Apache Tomcat servlet/JSP container default files (OID: 1.3.6.1.4.1.25623.1.0.12085)

```
Default files, such as documentation, default Servlets and JSPs were found on
the Apache Tomcat servlet/JSP container.

Remove default files, example JSPs and Servlets from the Tomcat
Servlet/JSP container.

These files should be removed as they may help an attacker to guess the
exact version of Apache Tomcat which is running on this host and may provide
other useful information.

The following default files were found :
/examples/servlets/index.html
/examples/jsp/snp/snoop.jsp
/examples/jsp/index.html
```

High (CVSS: 6.8) imap (143/tcp)
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check) (OID: 1.3.6.1.4.1.25623.1.0.105043)

Summary:
OpenSSL is prone to security-bypass vulnerability.

Result:
Vulnerability detected.

Impact

Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution

Updates are available.

Vulnerability Insight

OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method

Send two SSL ChangeCipherSpec request and check the response.

References

CVE: CVE-2014-0224
BID: 67899
CERT: DFN-CERT-2014-1364 , DFN-CERT-2014-1357 , DFN-CERT-2014-1350 , DFN-CERT-2014-1265 , DFN-CERT-2014-1209 , DFN-CERT-2014-0917 , DFN-CERT-2014-0789 , DFN-CERT-2014-0778 , DFN-CERT-2014-0768 , DFN-CERT-2014-0752 , DFN-CERT-2014-0747 , DFN-CERT-2014-0738 , DFN-CERT-2014-0715 , DFN-CERT-2014-0714 , DFN-CERT-2014-0709
Other: http://www.securityfocus.com/bid/67899
http://openssl.org/

High (CVSS: 6.8) pop3 (110/tcp)
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check) (OID: 1.3.6.1.4.1.25623.1.0.105043)

Summary:
OpenSSL is prone to security-bypass vulnerability.

Result:
Vulnerability detected.

Impact

Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a

man-in-the-middle attack. This may lead to other attacks.

Solution

Updates are available.

Vulnerability Insight

OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method

Send two SSL ChangeCipherSpec request and check the response.

References

CVE: CVE-2014-0224

BID: 67899

CERT: DFN-CERT-2014-1364 , DFN-CERT-2014-1357 , DFN-CERT-2014-1350 , DFN-CERT-2014-1265 , DFN-CERT-2014-1209 , DFN-CERT-2014-0917 , DFN-CERT-2014-0789 , DFN-CERT-2014-0778 , DFN-CERT-2014-0768 , DFN-CERT-2014-0752 , DFN-CERT-2014-0747 , DFN-CERT-2014-0738 , DFN-CERT-2014-0715 , DFN-CERT-2014-0714 , DFN-CERT-2014-0709

Other: http://www.securityfocus.com/bid/67899
http://openssl.org/

Medium (CVSS: 2.6) general/tcp
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Result:

```
It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 363780014
Paket 2: 363780122
```

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in

their synchronize (SYN) segment.

See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

References

Other: http://www.ietf.org/rfc/rfc1323.txt

Medium (CVSS: 4.3) imaps (993/tcp)
NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

```
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
```

Medium (CVSS: 4.3) pop3s (995/tcp)
NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

```
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
```

```
SSL3_ADH_DES_40_CBC_SHA
TLS1_RSA_RC4_40_MD5
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS1_RSA_RC2_40_MD5
TLS1_RSA_DES_40_CBC_SHA
TLS1_EDH_RSA_DES_40_CBC_SHA
TLS1_ADH_RC4_40_MD5
TLS1_ADH_RC4_128_MD5
TLS1_ADH_DES_40_CBC_SHA
```

Back to summary

Greenbone Security Assistant (GSA) Copyright 2009-2013 by Greenbone Networks GmbH, www.greenbone.net