Greenbone Security Assistant

<> Logged in as User **LabGroup68** | Logout

Wed Feb 21 10:58:49 2018 UTC

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

Administration **Help**

Report Summary

√Apply overrides

Result of Task:	**full system vulnerability csec068 - rome.nsec**
Order of results:	by host
Scan started:	**Wed Feb 21 09:31:11 2018**
Scan ended:	Wed Feb 21 09:48:15 2018
Scan status:	Done

Task

	High	Medium	Low	Log	False Pos.	**Total**	**Run Alert**	**Download**
Full report:	4	9	1	77	0	91		PDF
All filtered results:	4	9	0	0	0	13		PDF
Filtered results 1 - 13:	4	9	0	0	0	13		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

☑ Show notes

☑ 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 - 13 of 13

Host	OS	Start	End	High	Medium	Low	Log	False Pos.	Total
192.168.1.10 (rome.secnet)		Feb 21, 09:31:17	Feb 21, 09:48:15	4	9	0	0	0	13
Total: 1				4	9	0	0	0	13

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
http (80/tcp)	Medium
imaps (993/tcp)	Medium
microsoft-ds (445/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: 6.4) http-alt (8080/tcp)
NVT: Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service ... (OID: 1.3.6.1.4.1.25623.1.0.100712)

```
 Summary:
 Apache Tomcat is prone to multiple remote vulnerabilities including
information-disclosure and denial-of-service issues.

Remote attackers can exploit these issues to cause denial-of-service
conditions or gain access to potentially sensitive information;
information obtained may lead to further attacks.

The following versions are affected:

Tomcat 5.5.0 to 5.5.29 Tomcat 6.0.0 to 6.0.27 Tomcat 7.0.0

Tomcat 3.x, 4.x, and 5.0.x may also be affected.
 Solution:
 The vendor released updates. Please see the references for more
information.
```

Product Detection Result

Product: cpe:/a:apache:tomcat:6.0.24
Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
Details: View details of product detection

References

CVE: CVE-2010-2227
BID: 41544
CERT: DFN-CERT-2012-1832 , DFN-CERT-2012-0828 , DFN-CERT-2011-0465 , DFN-CERT-2011-0185 , DFN-CERT-2010-1647 , DFN-CERT-2010-1607 , DFN-CERT-2010-1560 , DFN-CERT-2010-1472 , DFN-CERT-2010-1247 , DFN-CERT-2010-1192 , DFN-CERT-2010-1190 , DFN-CERT-2010-0986 , DFN-CERT-2010-0985 , DFN-CERT-2010-0983
Other: https://www.securityfocus.com/bid/41544
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html
http://tomcat.apache.org/security-7.html
http://tomcat.apache.org/
http://www.securityfocus.com/archive/1/512272

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: 370915249
Paket 2: 370915357
```

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) http (80/tcp)
NVT: Apache Web Server ETag Header Information Disclosure Weakness (OID: 1.3.6.1.4.1.25623.1.0.103122)

```
Information that was gathered:
Inode: 152086
Size: 177
```

References

CVE: CVE-2003-1418
BID: 6939
Other: https://www.securityfocus.com/bid/6939
http://httpd.apache.org/docs/mod/core.html#fileetag
http://www.openbsd.org/errata32.html
http://support.novell.com/docs/Tids/Solutions/10090670.html

Medium (CVSS: 4.3) http (80/tcp)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902830)

```
  Summary:
  This host is running Apache HTTP Server and is prone to cookie
  information disclosure vulnerability.

  Vulnerability Insight:
  The flaw is due to an error within the default error response for
  status code 400 when no custom ErrorDocument is configured, which can be
  exploited to expose 'httpOnly' cookies.

  Impact:
  Successful exploitation will allow attackers to obtain sensitive information
  that may aid in further attacks.
  Impact Level: Application

  Affected Software/OS:
  Apache HTTP Server versions 2.2.0 through 2.2.21

  Solution:
  Upgrade to Apache HTTP Server version 2.2.22 or later,
  For updates refer to http://httpd.apache.org/
```

References

CVE: CVE-2012-0053

BID: 51706

CERT: DFN-CERT-2014-1592 , DFN-CERT-2014-0635 , DFN-CERT-2013-1307 , DFN-CERT-2012-1276 , DFN-CERT-2012-1112 , DFN-CERT-2012-0928 , DFN-CERT-2012-0758 , DFN-CERT-2012-0744 , DFN-CERT-2012-0568 , DFN-CERT-2012-0425 , DFN-CERT-2012-0424 , DFN-CERT-2012-0387 , DFN-CERT-2012-0343 , DFN-CERT-2012-0332 , DFN-CERT-2012-0306 , DFN-CERT-2012-0264 , DFN-CERT-2012-0203 , DFN-CERT-2012-0188

Other: http://osvdb.org/78556
http://secunia.com/advisories/47779
http://www.exploit-db.com/exploits/18442
http://rhn.redhat.com/errata/RHSA-2012-0128.html
http://httpd.apache.org/security/vulnerabilities_22.html
http://svn.apache.org/viewvc?view=revision&amp;revision=1235454
http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html

Medium (CVSS: 4.3) http-alt (8080/tcp)
NVT: Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilit... (OID: 1.3.6.1.4.1.25623.1.0.103032)

```
 Summary:
 Apache Tomcat is prone to multiple cross-site scripting
vulnerabilities because it fails to properly sanitize user-
supplied input.

An attacker may leverage these issues to execute arbitrary script code
in the browser of an unsuspecting user in the context of the affected
site. This may let the attacker steal cookie-based authentication
credentials and launch other attacks.
 Solution:
 Updates are available; please see the references for more information.
```

Product Detection Result

Product: cpe:/a:apache:tomcat:6.0.24
Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
Details: View details of product detection

References

CVE: CVE-2010-4172
BID: 45015
CERT: DFN-CERT-2012-1832 , DFN-CERT-2011-0793 , DFN-CERT-2011-0181
Other: https://www.securityfocus.com/bid/45015
http://tomcat.apache.org/security-6.html
http://tomcat.apache.org/security-7.html
http://tomcat.apache.org/security-6.html
http://tomcat.apache.org/security-7.html
http://jakarta.apache.org/tomcat/
http://www.securityfocus.com/archive/1/514866

Medium (CVSS: 2.6) http-alt (8080/tcp)
NVT: Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerabi... (OID: 1.3.6.1.4.1.25623.1.0.100598)

```
 Summary:
 Apache Tomcat is prone to a remote information-disclosure
vulnerability.

Remote attackers can exploit this issue to obtain the host name or IP
address of the Tomcat server. Information harvested may lead to
further attacks.

The following versions are affected:

Tomcat 5.5.0 through 5.5.29 Tomcat 6.0.0 through 6.0.26

Tomcat 3.x, 4.0.x, and 5.0.x may also be affected.
 Solution:
 Updates are available. Please see the references for more information.
```

Product Detection Result

Product:	cpe:/a:apache:tomcat:6.0.24
Method:	Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
Details:	View details of product detection

References

CVE:	CVE-2010-1157
BID:	39635
CERT:	DFN-CERT-2012-1832 , DFN-CERT-2011-0465 , DFN-CERT-2011-0185 , DFN-CERT-2010-1647 , DFN-CERT-2010-1607 , DFN-CERT-2010-1247 , DFN-CERT-2010-1192 , DFN-CERT-2010-1190
Other:	http://www.securityfocus.com/bid/39635 http://tomcat.apache.org/security-5.html http://tomcat.apache.org/security-6.html http://tomcat.apache.org/ http://svn.apache.org/viewvc?view=revision&amp;revision=936540 http://svn.apache.org/viewvc?view=revision&amp;revision=936541 http://www.securityfocus.com/archive/1/510879

Medium (CVSS: 2.6) http-alt (8080/tcp)
NVT: Apache Tomcat Security bypass vulnerability (OID: 1.3.6.1.4.1.25623.1.0.901114)

```
  Summary:
  This host is running Apache Tomcat server and is prone to security
  bypass vulnerability.

  Vulnerability Insight:
  The flaw is caused by 'realm name' in the 'WWW-Authenticate' HTTP header for
  'BASIC' and 'DIGEST' authentication that might allow remote attackers to
  discover the server's hostname or IP address by sending a request for a
  resource.

  Impact:
  Remote attackers can exploit this issue to obtain the host name or IP address
  of the Tomcat server. Information harvested may aid in further attacks.
  Impact Level: Application

  Affected Software/OS:
  Apache Tomcat version 5.5.0 to 5.5.29
  Apache Tomcat version 6.0.0 to 6.0.26

  Solution:
  Upgrade to the latest version of Apache Tomcat 5.5.30 or 6.0.27 or later,
  For updates refer to http://tomcat.apache.org
```

Product Detection Result

Product:	cpe:/a:apache:tomcat:6.0.24
Method:	Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
Details:	View details of product detection

References

CVE:	CVE-2010-1157
BID:	39635
CERT:	DFN-CERT-2012-1832 , DFN-CERT-2011-0465 , DFN-CERT-2011-0185 , DFN-CERT-2010-1647 , DFN-CERT-2010-1607 , DFN-CERT-2010-1247 , DFN-CERT-2010-1192 , DFN-CERT-2010-1190
Other:	http://tomcat.apache.org/security-5.html http://tomcat.apache.org/security-6.html http://www.securityfocus.com/archive/1/510879

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: 5.0) microsoft-ds (445/tcp)
NVT: Samba Multiple Remote Denial of Service Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.100644)

```
 Summary:
 Samba is prone to multiple remote denial-of-service vulnerabilities.

An attacker can exploit these issues to crash the application, denying
service to legitimate users.

Versions prior to Samba 3.4.8 and 3.5.2 are vulnerable.
 Solution:
 Updates are available. Please see the references for more information.
```

References

CVE:	CVE-2010-1635
BID:	40097
CERT:	DFN-CERT-2010-0954
Other:	http://www.securityfocus.com/bid/40097
	https://bugzilla.samba.org/show_bug.cgi?id=7254
	http://samba.org/samba/history/samba-3.4.8.html
	http://samba.org/samba/history/samba-3.5.2.html
	http://www.samba.org

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