

# Scan Report

February 16, 2018

## Summary

This document reports on the results of an automatic security scan. The scan started at Fri Feb 16 14:32:39 2018 UTC and ended at Fri Feb 16 14:58:46 2018 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

<b>1</b>	<b>Result Overview</b>	<b>2</b>
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	192.168.1.10 . . . . .	2
2.1.1	High http (80/tcp) . . . . .	2
2.1.2	High http-alt (8080/tcp) . . . . .	3
2.1.3	High imap (143/tcp) . . . . .	4
2.1.4	High imaps (993/tcp) . . . . .	5
2.1.5	High pop3 (110/tcp) . . . . .	5
2.1.6	High pop3s (995/tcp) . . . . .	6
2.1.7	Medium http (80/tcp) . . . . .	6
2.1.8	Medium http-alt (8080/tcp) . . . . .	8
2.1.9	Medium imaps (993/tcp) . . . . .	10
2.1.10	Medium pop3s (995/tcp) . . . . .	11
2.1.11	Medium general/tcp . . . . .	13
2.1.12	Medium netbios-ssn (139/tcp) . . . . .	13
2.1.13	Medium ssh (22/tcp) . . . . .	14

## 1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.1.10 (rome.secnet)	Severity: High	7	14	0	0	0
Total: 1		7	14	0	0	0

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Notes are included in the report.

This report might not show details of all issues that were found.

It only lists hosts that produced issues.

Issues with the threat level "Low" are not shown.

Issues with the threat level "Log" are not shown.

Issues with the threat level "Debug" are not shown.

Issues with the threat level "False Positive" are not shown.

This report contains all 21 results selected by the filtering described above. Before filtering there were 85 results.

## 2 Results per Host

### 2.1 192.168.1.10

Host scan start Fri Feb 16 14:32:45 2018 UTC

Host scan end Fri Feb 16 14:58:46 2018 UTC

Service (Port)	Threat Level
http (80/tcp)	High
http-alt (8080/tcp)	High
imap (143/tcp)	High
imaps (993/tcp)	High
pop3 (110/tcp)	High
pop3s (995/tcp)	High
http (80/tcp)	Medium
http-alt (8080/tcp)	Medium
imaps (993/tcp)	Medium
pop3s (995/tcp)	Medium
general/tcp	Medium
netbios-ssn (139/tcp)	Medium
ssh (22/tcp)	Medium

#### 2.1.1 High http (80/tcp)

### High (CVSS: 10.0) NVT: Apache Multiple Security Vulnerabilities

#### Summary:

Apache is prone to multiple vulnerabilities.  
These issues may lead to information disclosure or other attacks.  
Apache versions prior to 2.2.15 are affected.

#### Solution:

Upgrade to Apache 2.2.15 or Later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100514

#### References

CVE: CVE-2010-0425, CVE-2010-0434, CVE-2010-0408, CVE-2007-6750

BID:38494, 38491

#### Other:

URL:<http://www.securityfocus.com/bid/38494>

URL:[http://httpd.apache.org/security/vulnerabilities\\_22.html](http://httpd.apache.org/security/vulnerabilities_22.html)

URL:<http://httpd.apache.org/>

URL:[https://issues.apache.org/bugzilla/show\\_bug.cgi?id=48359](https://issues.apache.org/bugzilla/show_bug.cgi?id=48359)

URL:<http://svn.apache.org/viewvc?view=revision&revision=917870>

[\[ return to 192.168.1.10 \]](#)

### 2.1.2 High http-alt (8080/tcp)

### High (CVSS: 6.8) NVT: Apache Tomcat servlet/JSP container default files

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.12085

High (CVSS: 6.4)

NVT: Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service Vulnerabilities

#### Product detection result

cpe:/a:apache:tomcat:6.0.24

Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

#### 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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100712

#### References

CVE: CVE-2010-2227

BID:41544

#### Other:

URL:<https://www.securityfocus.com/bid/41544>

URL:<http://tomcat.apache.org/security-5.html>

URL:<http://tomcat.apache.org/security-6.html>

URL:<http://tomcat.apache.org/security-7.html>

URL:<http://tomcat.apache.org/>

URL:<http://www.securityfocus.com/archive/1/512272>

[\[ return to 192.168.1.10 \]](#)

### 2.1.3 High imap (143/tcp)

High (CVSS: 6.8)

NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)

... continues on next page ...

...continued from previous page ...
OID of test routine: 1.3.6.1.4.1.25623.1.0.105043
<b>References</b> CVE: CVE-2014-0224 BID:67899 Other: URL:http://www.securityfocus.com/bid/67899 URL:http://openssl.org/

[\[ return to 192.168.1.10 \]](#)

#### 2.1.4 High imaps (993/tcp)

High (CVSS: 6.8) NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
OID of test routine: 1.3.6.1.4.1.25623.1.0.105042
<b>References</b> CVE: CVE-2014-0224 BID:67899 Other: URL:http://www.securityfocus.com/bid/67899 URL:http://openssl.org/

[\[ return to 192.168.1.10 \]](#)

#### 2.1.5 High pop3 (110/tcp)

High (CVSS: 6.8) NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)
OID of test routine: 1.3.6.1.4.1.25623.1.0.105043
... continues on next page ...

...continued from previous page ...

**References**

CVE: CVE-2014-0224

BID:67899

Other:

URL:http://www.securityfocus.com/bid/67899

URL:http://openssl.org/

[\[ return to 192.168.1.10 \]](#)**2.1.6 High pop3s (995/tcp)**

High (CVSS: 6.8)

NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

OID of test routine: 1.3.6.1.4.1.25623.1.0.105042

**References**

CVE: CVE-2014-0224

BID:67899

Other:

URL:http://www.securityfocus.com/bid/67899

URL:http://openssl.org/

[\[ return to 192.168.1.10 \]](#)**2.1.7 Medium http (80/tcp)**

Medium (CVSS: 4.3)

NVT: Apache Web Server ETag Header Information Disclosure Weakness

Information that was gathered:

Inode: 152086

Size: 177

OID of test routine: 1.3.6.1.4.1.25623.1.0.103122

**References**

... continues on next page ...

...continued from previous page ...

CVE: CVE-2003-1418

BID:6939

Other:

URL:<https://www.securityfocus.com/bid/6939>

URL:<http://httpd.apache.org/docs/mod/core.html#fileetag>

URL:<http://www.openbsd.org/errata32.html>

URL:<http://support.novell.com/docs/Tids/Solutions/10090670.html>

Medium (CVSS: 4.3)

NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

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/>

OID of test routine: 1.3.6.1.4.1.25623.1.0.902830

## References

CVE: CVE-2012-0053

BID:51706

Other:

URL:<http://osvdb.org/78556>

URL:<http://secunia.com/advisories/47779>

URL:<http://www.exploit-db.com/exploits/18442>

URL:<http://rhn.redhat.com/errata/RHSA-2012-0128.html>

URL:[http://httpd.apache.org/security/vulnerabilities\\_22.html](http://httpd.apache.org/security/vulnerabilities_22.html)

URL:<http://svn.apache.org/viewvc?view=revision&revision=1235454>

URL:<http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm>

↪1

[ [return to 192.168.1.10](#) ]

## 2.1.8 Medium http-alt (8080/tcp)

Medium (CVSS: 4.3) NVT: Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilities
<b>Product detection result</b> cpe:/a:apache:tomcat:6.0.24 Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
<p>Summary:</p> <p>Apache Tomcat is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.</p> <p>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.</p> <p>Solution:</p> <p>Updates are available; please see the references for more information.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.103032</p>
<b>References</b> CVE: CVE-2010-4172 BID:45015 Other: URL: <a href="https://www.securityfocus.com/bid/45015">https://www.securityfocus.com/bid/45015</a> URL: <a href="http://tomcat.apache.org/security-6.html">http://tomcat.apache.org/security-6.html</a> URL: <a href="http://tomcat.apache.org/security-7.html">http://tomcat.apache.org/security-7.html</a> URL: <a href="http://tomcat.apache.org/security-6.html">http://tomcat.apache.org/security-6.html</a> URL: <a href="http://tomcat.apache.org/security-7.html">http://tomcat.apache.org/security-7.html</a> URL: <a href="http://jakarta.apache.org/tomcat/">http://jakarta.apache.org/tomcat/</a> URL: <a href="http://www.securityfocus.com/archive/1/514866">http://www.securityfocus.com/archive/1/514866</a>

Medium (CVSS: 2.6) NVT: Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability
<b>Product detection result</b> cpe:/a:apache:tomcat:6.0.24 Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
<p>Summary:</p> <p>... continues on next page ...</p>



...continued from previous page ...

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100598

#### References

CVE: CVE-2010-1157

BID:39635

Other:

URL:<http://www.securityfocus.com/bid/39635>

URL:<http://tomcat.apache.org/security-5.html>

URL:<http://tomcat.apache.org/security-6.html>

URL:<http://tomcat.apache.org/>

URL:<http://svn.apache.org/viewvc?view=revision&revision=936540>

URL:<http://svn.apache.org/viewvc?view=revision&revision=936541>

URL:<http://www.securityfocus.com/archive/1/510879>

Medium (CVSS: 2.6)

NVT: Apache Tomcat Security bypass vulnerability

#### Product detection result

cpe:/a:apache:tomcat:6.0.24

Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

#### 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.

...continues on next page ...

<p>...continued from previous page ...</p> <p>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 <a href="http://tomcat.apache.org">http://tomcat.apache.org</a></p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.901114</p>
<p><b>References</b>  CVE: CVE-2010-1157  BID:39635  Other:  URL:<a href="http://tomcat.apache.org/security-5.html">http://tomcat.apache.org/security-5.html</a>  URL:<a href="http://tomcat.apache.org/security-6.html">http://tomcat.apache.org/security-6.html</a>  URL:<a href="http://www.securityfocus.com/archive/1/510879">http://www.securityfocus.com/archive/1/510879</a></p>

[\[ return to 192.168.1.10 \]](#)

### 2.1.9 Medium imaps (993/tcp)

<p>Medium (CVSS: 4.3)  NVT: Check for SSL Weak Ciphers</p>
<p>Weak ciphers offered by this service:</p> <ul style="list-style-type: none"> <li>SSL3_RSA_RC4_40_MD5</li> <li>SSL3_RSA_RC4_128_MD5</li> <li>SSL3_RSA_RC4_128_SHA</li> <li>SSL3_RSA_RC2_40_MD5</li> <li>SSL3_RSA_DES_40_CBC_SHA</li> <li>SSL3_EDH_RSA_DES_40_CBC_SHA</li> <li>SSL3_ADH_RC4_40_MD5</li> <li>SSL3_ADH_RC4_128_MD5</li> <li>SSL3_ADH_DES_40_CBC_SHA</li> <li>TLS1_RSA_RC4_40_MD5</li> <li>TLS1_RSA_RC4_128_MD5</li> <li>TLS1_RSA_RC4_128_SHA</li> <li>TLS1_RSA_RC2_40_MD5</li> <li>TLS1_RSA_DES_40_CBC_SHA</li> <li>TLS1_EDH_RSA_DES_40_CBC_SHA</li> <li>TLS1_ADH_RC4_40_MD5</li> <li>TLS1_ADH_RC4_128_MD5</li> </ul> <p>... continues on next page ...</p>

<p>...continued from previous page ...</p> <p>TLS1_ADH_DES_40_CBC_SHA</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.103440</p>
--

<p>Medium (CVSS: 4.3)</p> <p>NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.802087</p> <p><b>References</b></p> <p>CVE: CVE-2014-3566</p> <p>BID:70574</p> <p>Other:</p> <p>URL:<a href="http://osvdb.com/113251">http://osvdb.com/113251</a></p> <p>URL:<a href="https://www.openssl.org/~bodo/ssl-poodle.pdf">https://www.openssl.org/~bodo/ssl-poodle.pdf</a></p> <p>URL:<a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a></p> <p>URL:<a href="https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html">https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html</a></p> <p>URL:<a href="http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit-ing-ssl-30.html">http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit-ing-ssl-30.html</a></p>
--

<p>Medium (CVSS: 0.0)</p> <p>NVT: SSL Certificate Expiry</p> <p>The SSL certificate of the remote service expired 2015-12-04 15:16:06 GMT!</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.15901</p>
--

[\[ return to 192.168.1.10 \]](#)

### 2.1.10 Medium pop3s (995/tcp)

<p>Medium (CVSS: 4.3)</p> <p>NVT: Check for SSL Weak Ciphers</p> <p>Weak ciphers offered by this service:</p> <p>SSL3_RSA_RC4_40_MD5</p> <p>...continues on next page ...</p>
---

...continued from previous page ...

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

Medium (CVSS: 4.3)

NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

OID of test routine: 1.3.6.1.4.1.25623.1.0.802087

**References**

CVE: CVE-2014-3566

BID: 70574

**Other:**URL: <http://osvdb.com/113251>URL: <https://www.openssl.org/~bodo/ssl-poodle.pdf>URL: <https://www.imperialviolet.org/2014/10/14/poodle.html>URL: <https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html>
 URL: [http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit-  
ing-ssl-30.html](http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit-ing-ssl-30.html)

Medium (CVSS: 0.0)

NVT: SSL Certificate Expiry

...continues on next page ...

...continued from previous page ...
The SSL certificate of the remote service expired 2015-12-04 15:16:06 GMT!
OID of test routine: 1.3.6.1.4.1.25623.1.0.15901

[\[ return to 192.168.1.10 \]](#)

### 2.1.11 Medium general/tcp

Medium (CVSS: 2.6) NVT: TCP timestamps
<p>It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 329526152 Paket 2: 329526258</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.80091</p>
<b>References</b> Other: URL: <a href="http://www.ietf.org/rfc/rfc1323.txt">http://www.ietf.org/rfc/rfc1323.txt</a>

[\[ return to 192.168.1.10 \]](#)

### 2.1.12 Medium netbios-ssn (139/tcp)

Medium (CVSS: 5.0) NVT: Samba Multiple Remote Denial of Service Vulnerabilities
<p><b>Summary:</b> 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. <b>Solution:</b> Updates are available. Please see the references for more information.</p>
...continues on next page ...

...continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.100644

**References**

CVE: CVE-2010-1635

BID:40097

Other:

URL:<http://www.securityfocus.com/bid/40097>URL:[https://bugzilla.samba.org/show\\_bug.cgi?id=7254](https://bugzilla.samba.org/show_bug.cgi?id=7254)URL:<http://samba.org/samba/history/samba-3.4.8.html>URL:<http://samba.org/samba/history/samba-3.5.2.html>URL:<http://www.samba.org>[\[ return to 192.168.1.10 \]](#)**2.1.13 Medium ssh (22/tcp)**

Medium (CVSS: 3.5)

NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability

According to its banner, the version of OpenSSH installed on the remote host is older than 5.7:

```
ssh-2.0-openssh_5.3p1 debian-3ubuntu7
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103503

**References**

CVE: CVE-2012-0814

BID:51702

Other:

URL:<http://www.securityfocus.com/bid/51702>URL:<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445>URL:<http://packages.debian.org/squeeze/openssh-server>URL:<https://downloads.avaya.com/css/P8/documents/100161262>[\[ return to 192.168.1.10 \]](#)