Scan Report

February 21, 2018

Summary

This document reports on the results of an automatic security scan. The scan started at Wed Feb 21 09:31:11 2018 UTC and ended at Wed Feb 21 09:48:15 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

1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.1.10 (rome.secnet)	Severity: High	4	9	0	0	0
Total: 1		4	9	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 13 results selected by the filtering described above. Before filtering there were 92 results.

2 Results per Host

2.1 192.168.1.10

Host scan start	Wed Feb 21 09:31:17 2018 UTC
Host scan end	Wed Feb 21 09:48:15 2018 UTC

Service (Port)	Threat Level
http-alt (8080/tcp)	High
imap (143/tcp)	High
pop3 (110/tcp)	High
http-alt (8080/tcp)	Medium
general/tcp	Medium
http (80/tcp)	Medium
imaps (993/tcp)	Medium
microsoft-ds (445/tcp)	Medium
pop3s (995/tcp)	Medium

2.1.1 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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
    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]

2.1.2 High imap (143/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

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]

2.1.3 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

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]

2.1.4 Medium http-alt (8080/tcp)

Medium (CVSS: 4.3)
NVT: Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting 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 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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103032

References

```
CVE: CVE-2010-4172
BID:45015
Other:
  URL:https://www.securityfocus.com/bid/45015
   URL:http://tomcat.apache.org/security-6.html
   URL:http://tomcat.apache.org/security-7.html
   URL:http://tomcat.apache.org/security-6.html
   URL:http://tomcat.apache.org/security-7.html
   URL:http://jakarta.apache.org/tomcat/
   URL:http://www.securityfocus.com/archive/1/514866
```

Medium (CVSS: 2.6)
NVT: Apache Tomcat Authentication Header Realm Name Information Disclosure 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)
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
 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.
```

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&amp;revision=936540
   URL:http://svn.apache.org/viewvc?view=revision&amp;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.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.901114

References

```
CVE: CVE-2010-1157
BID:39635
Other:
  URL:http://tomcat.apache.org/security-5.html
   URL:http://tomcat.apache.org/security-6.html
   URL:http://www.securityfocus.com/archive/1/510879
```

[return to 192.168.1.10]

2.1.5 Medium general/tcp

Medium (CVSS: 2.6)
NVT: TCP timestamps

```
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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

References

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

[return to 192.168.1.10]

2.1.6 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

```
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

. . . continues on next page . . .

. . . continued from previous page . . .

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
   URL:http://svn.apache.org/viewvc?view=revision&amp;revision=1235454
   URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l
```

[return to 192.168.1.10]

2.1.7 Medium imaps (993/tcp)

Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers

```
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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

[return to 192.168.1.10]

2.1.8 Medium microsoft-ds (445/tcp)

Medium (CVSS: 5.0)
NVT: Samba Multiple Remote Denial of Service Vulnerabilities

```
 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.
```

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
   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]

2.1.9 Medium pop3s (995/tcp)

Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers

```
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
   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

[return to 192.168.1.10]