Scan Report

August 31, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 192.168.56.102". The scan started at Sun Aug 31 17:10:33 2025 UTC and ended at Sun Aug 31 18:08:51 2025 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	High	Medium	Low	Log	False Positive
192.168.56.102	13	0	0	0	0
Total: 1	13	0	0	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
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.
Only results with a minimum QoD of 70 are shown.

This report contains all 13 results selected by the filtering described above. Before filtering there were 618 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.56.102	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.56.102

Host scan start Sun Aug 31 17:14:37 2025 UTC
Host scan end Sun Aug 31 18:08:46 2025 UTC

Service (Port)	Threat Level
512/tcp	High
80/tcp	High
general/tcp	High
3632/tcp	High
6200/tcp	High
1524/tcp	High
21/tcp	High
8009/tcp	High
513/tcp	High

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
8787/tcp	High
3306/tcp	High

2.1.1 High 512/tcp

High (CVSS: 10.0)
NVT: The rexec service is running

Summary
This remote host is running a rexec service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The rexec service was detected on the target system.`

Solution:
Solution type: Mitigation
Disable the rexec service and use alternatives like SSH instead.

Vulnerability Insight
rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.
The main difference is that rexec authenticate by reading the username and password *unencrypted* from the socket.

Vulnerability Detection Method
Checks whether an rexec service is exposed on the target host.
Details: `The rexec service is running`
OID:1.3.6.1.4.1.25623.1.0.100111
Version used: `2023-09-12T05:05:19Z`

References
`cve: CVE-1999-0618`

[return to 192.168.56.102]

2.1.2 High 80/tcp

High (CVSS: 10.0)
NVT: TWiki XSS and Command Execution Vulnerabilities

... continues on next page ...

... continued from previous page ...

Summary
TWiki is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 4.2.4`

Impact
Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.

Solution:
Solution type: VendorFix
Upgrade to version 4.2.4 or later.

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight
The flaws are due to:
- %URLPARAM}}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.
- %SEARCH}}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details: `TWiki XSS and Command Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: `2024-03-01T14:37:10Z`

References
`cve: CVE-2008-5304`
`cve: CVE-2008-5305`
`url: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304`
`url: http://www.securityfocus.com/bid/32668`
`url: http://www.securityfocus.com/bid/32669`
`url: http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305`

High (CVSS: 9.8)
NVT: PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check

Summary
PHP is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 95%

Vulnerability Detection Result

```
By doing the following HTTP POST request:
"HTTP POST" body : <?php phpinfo();?>
URL              : http://192.168.56.102/cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%7
↪5%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D
↪%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%
↪6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+
↪%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%
↪72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%6
↪3%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E
↪%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E
it was possible to execute the "<?php phpinfo();?>" command.
Result:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/cgi </td></tr>
  <h2>PHP Variables</h2>
```

Impact

Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.

Solution:

Solution type: VendorFix

PHP: Update to version 5.3.13, 5.4.3 or later

- Other products / applications: Please contact the vendor for a solution

Affected Software/OS

PHP versions prior to 5.3.13 and 5.4.x prior to 5.4.3.

Other products / applications might be affected by the tested CVE-2012-1823 as well.

Vulnerability Insight

When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.

An example of the -s command, allowing an attacker to view the source code of index.php is below:

http://example.com/index.php?-s

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Send multiple a crafted HTTP POST requests and checks the responses.
Note: This script checks for the presence of CVE-2012-1823 which indicates that the system is also affected by the other included CVEs.
Details: PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: 2025-04-24T05:40:00Z

References

cve: CVE-2012-1823
cve: CVE-2012-2311
cve: CVE-2012-2336
cve: CVE-2012-2335
url: https://web.archive.org/web/20190212080415/http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
url: https://www.kb.cert.org/vuls/id/520827
url: https://bugs.php.net/bug.php?id=61910
url: https://www.php.net/manual/en/security.cgi-bin.php
url: https://web.archive.org/web/20210121223743/http://www.securityfocus.com/bid/53388
url: https://web.archive.org/web/20120709064615/http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-risks-Update-2-1567532.html
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
cisa: Known Exploited Vulnerability (KEV) catalog
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-1316
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1268
dfn-cert: DFN-CERT-2012-1267
dfn-cert: DFN-CERT-2012-1266
dfn-cert: DFN-CERT-2012-1173
dfn-cert: DFN-CERT-2012-1101
dfn-cert: DFN-CERT-2012-0994
dfn-cert: DFN-CERT-2012-0993
dfn-cert: DFN-CERT-2012-0992
dfn-cert: DFN-CERT-2012-0920
dfn-cert: DFN-CERT-2012-0915
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0913
dfn-cert: DFN-CERT-2012-0907
dfn-cert: DFN-CERT-2012-0906
dfn-cert: DFN-CERT-2012-0900
dfn-cert: DFN-CERT-2012-0880
dfn-cert: DFN-CERT-2012-0878

High (CVSS: 9.8)
NVT: PHP < 5.6.30, 7.x < 7.0.15, 7.1.x < 7.1.1 Multiple Vulnerabilities (Jan 2017) - Linux

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.30
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.30, 7.0.15, 7.1.1 or later.

Affected Software/OS
PHP prior to version 5.6.30, 7.x prior to 7.0.15 and 7.1.x prior to 7.1.1.

Vulnerability Insight
The following flaws exist:
- CVE-2016-10161: Heap out of bounds read on unserialize in finish_nested_data()
- CVE-2016-10158: FPE when parsing a tag format
- CVE-2016-10168: Signed Integer Overflow gd_io.c
- CVE-2016-10167: DOS vulnerability in gdImageCreateFromGd2Ctx()
- CVE-2017-11147: Seg fault when loading hostile phar
- CVE-2016-10160: Memory corruption when loading hostile phar
- CVE-2016-10159: Crash while loading hostile phar archive

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 5.6.30, 7.x < 7.0.15, 7.1.x < 7.1.1 Multiple Vulnerabilities (Jan 2017) -.
↪..
OID:1.3.6.1.4.1.25623.1.0.108052
Version used: 2025-05-21T05:40:19Z

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Detection (HTTP)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

cve: CVE-2016-10158
cve: CVE-2016-10159
cve: CVE-2016-10160
cve: CVE-2016-10161
cve: CVE-2016-10167
cve: CVE-2016-10168
cve: CVE-2017-11147
url: http://www.php.net/ChangeLog-5.php
url: http://www.php.net/ChangeLog-7.php
url: http://bugs.php.net/73825
url: http://bugs.php.net/73737
url: http://bugs.php.net/73869
url: http://bugs.php.net/73868
url: http://bugs.php.net/73773
url: http://bugs.php.net/73768
url: http://bugs.php.net/73764
cert-bund: WID-SEC-2023-2718
cert-bund: CB-K17/1957
cert-bund: CB-K17/1575
cert-bund: CB-K17/1461
cert-bund: CB-K17/1358
cert-bund: CB-K17/1252
cert-bund: CB-K17/0527
cert-bund: CB-K17/0327
cert-bund: CB-K17/0318
cert-bund: CB-K17/0269
cert-bund: CB-K17/0264
cert-bund: CB-K17/0232
cert-bund: CB-K17/0182
cert-bund: CB-K17/0141
dfn-cert: DFN-CERT-2018-0835
dfn-cert: DFN-CERT-2017-2044
dfn-cert: DFN-CERT-2017-1647
dfn-cert: DFN-CERT-2017-1529
dfn-cert: DFN-CERT-2017-1420
dfn-cert: DFN-CERT-2017-1295
dfn-cert: DFN-CERT-2017-0532
dfn-cert: DFN-CERT-2017-0334
dfn-cert: DFN-CERT-2017-0325
dfn-cert: DFN-CERT-2017-0274
dfn-cert: DFN-CERT-2017-0270
dfn-cert: DFN-CERT-2017-0234
dfn-cert: DFN-CERT-2017-0179

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2017-0144

[return to 192.168.56.102]

2.1.3 High general/tcp

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

Product detection result
cpe:/o:canonical:ubuntu_linux:8.04
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)

Summary
The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The "Ubuntu" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP: 8.04
EOL date: 2013-05-09
EOL info: https://wiki.ubuntu.com/Releases

Impact
An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: Mitigation
Update the OS on the remote host to a version which is still supported and receiving security updates by the vendor.
Note / Important: Please create an override for this result if the target host is a:
- Windows system with Extended Security Updates (ESU)
- System with additional 3rd-party / non-vendor security updates like e.g. from 'TuxCare', 'Freexian Extended LTS' or similar

Vulnerability Detection Method
Checks if an EOL version of an OS is present on the target host.
Details: Operating System (OS) End of Life (EOL) Detection

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.103674
Version used: 2025-05-21T05:40:19Z

Product Detection Result
Product: cpe:/o:canonical:ubuntu_linux:8.04
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 192.168.56.102]

2.1.4 High 3632/tcp

High (CVSS: 9.3)
NVT: DistCC RCE Vulnerability (CVE-2004-2687)

Summary
DistCC is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
It was possible to execute the "id" command.
Result: uid=1(daemon) gid=1(daemon)

Impact
DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.

Solution:
Solution type: VendorFix
Vendor updates are available. Please see the references for more information.
For more information about DistCC's security see the references.

Vulnerability Insight
DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

Vulnerability Detection Method
Details: DistCC RCE Vulnerability (CVE-2004-2687)
OID:1.3.6.1.4.1.25623.1.0.103553
Version used: 2022-07-07T10:16:06Z

References

... continues on next page ...

... continued from previous page ...

cve: CVE-2004-2687
url: https://distcc.github.io/security.html
url: https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80
↪/archives/bugtraq/2005-03/0183.html
dfn-cert: DFN-CERT-2019-0381

[return to 192.168.56.102]

2.1.5 High 6200/tcp

High (CVSS: 9.8)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution:
Solution type: VendorFix
The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.

Vulnerability Insight
The tainted source package contains a backdoor which opens a shell on port 6200/tcp.

Vulnerability Detection Method
Details: vsftpd Compromised Source Packages Backdoor Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: 2023-12-07T05:05:41Z

References
cve: CVE-2011-2523
url: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backd

... continues on next page ...

... continued from previous page ...

```
↪oored.html
url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bi
↪d/48539/
url: https://security.appspot.com/vsftpd.html
```

[return to 192.168.56.102]

2.1.6 High 1524/tcp

High (CVSS: 10.0)
NVT: Possible Backdoor: Ingreslock

Summary
A backdoor is installed on the remote host.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
The service is answering to an 'id;' command with the following response: uid=0(
↪root) gid=0(root)
```

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Solution:
Solution type: Workaround
A whole cleanup of the infected system is recommended.

Vulnerability Detection Method
Details: `Possible Backdoor: Ingreslock`
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: `2023-07-25T05:05:58Z`

[return to 192.168.56.102]

2.1.7 High 21/tcp

High (CVSS: 9.8)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Product detection result

```
cpe:/a:beasts:vsftpd:2.3.4
```

... continues on next page ...

... continued from previous page ...

Detected by vsFTPd FTP Server Detection (OID: 1.3.6.1.4.1.25623.1.0.111050)

Summary
vsftpd is prone to a backdoor vulnerability.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution:
Solution type: VendorFix
The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.

Vulnerability Insight
The tainted source package contains a backdoor which opens a shell on port 6200/tcp.

Vulnerability Detection Method
Details: vsftpd Compromised Source Packages Backdoor Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: 2023-12-07T05:05:41Z

Product Detection Result
Product: cpe:/a:beasts:vsftpd:2.3.4
Method: vsFTPd FTP Server Detection
OID: 1.3.6.1.4.1.25623.1.0.111050)

References
cve: CVE-2011-2523
url: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backd
↪oored.html
url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bi
↪d/48539/
url: https://security.appspot.com/vsftpd.html

[return to 192.168.56.102]

2.1.8 High 8009/tcp

High (CVSS: 9.8)
NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check

Summary
Apache Tomcat is prone to a remote code execution (RCE) vulnerability in the AJP connector dubbed 'Ghostcat'.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.
Result:
AB 8\x0004 Ã\x0088 \x0002OK  \x0001 \x000CContent-Type  \x001Ctext/html;charset=
↪ISO-8859-1 AB\x001FÃ¼\x0003\x001FÃ¸<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at
      http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
    <head>
    <title>Apache Tomcat/5.5</title>
    <style type="text/css">
    /*<![CDATA[*/
      body {
          color: #000000;
          background-color: #FFFFFF;
   font-family: Arial, "Times New Roman", Times, serif;
          margin: 10px 0px;
      }
    img {
       border: none;
    }

    a:link, a:visited {
```

... continues on next page ...

... continued from previous page ...

```
        color: blue
    }
    th {
        font-family: Verdana, "Times New Roman", Times, serif;
        font-size: 110%;
        font-weight: normal;
        font-style: italic;
        background: #D2A41C;
        text-align: left;
    }
    td {
        color: #000000;
 font-family: Arial, Helvetica, sans-serif;
    }

    td.menu {
        background: #FFDC75;
    }
    .center {
        text-align: center;
    }
    .code {
        color: #000000;
        font-family: "Courier New", Courier, monospace;
        font-size: 110%;
        margin-left: 2.5em;
    }

     #banner {
        margin-bottom: 12px;
     }
     p#congrats {
         margin-top: 0;
         font-weight: bold;
         text-align: center;
     }
     p#footer {
         text-align: right;
         font-size: 80%;
     }
     /*]]>*/
   </style>
</head>
<body>
<!-- Header -->
<table id="banner" width="100%">
    <tr>
```

... continues on next page ...

. . . continued from previous page . . .

```
      <td align="left" style="width:130px">
        <a href="http://tomcat.apache.org/">
   <img src="tomcat.gif" height="92" width="130" alt="The Mighty Tomcat - MEOW!"
↪/>
 </a>
      </td>
      <td align="left" valign="top"><b>Apache Tomcat/5.5</b></td>
      <td align="right">
        <a href="http://www.apache.org/">
   <img src="asf-logo-wide.gif" height="51" width="537" alt="The Apache Software
↪ Foundation"/>
 </a>
       </td>
     </tr>
</table>
<table>
    <tr>
        <!-- Table of Contents -->
        <td valign="top">
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
   <th>Administration</th>
                </tr>
                <tr>
   <td class="menu">
     <a href="manager/status">Status</a><br/>
                    <a href="admin">Tomcat Administration</a><br/>
                    <a href="manager/html">Tomcat Manager</a><br/>
                     
                  </td>
                </tr>
            </table>
     <br />
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
   <th>Documentation</th>
                </tr>
                <tr>
                  <td class="menu">
                    <a href="RELEASE-NOTES.txt">Release Notes</a><br/>
                    <a href="tomcat-docs/changelog.html">Change Log</a><br/
↪>
                    <a href="tomcat-docs">Tomcat Documentation</a><br/>
↪                      
                     
     </td>
                </tr>
```

. . . continues on next page . . .

... continued from previous page ...

```
            </table>

            <br/>
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
                  <th>Tomcat Online</th>
                </tr>
                <tr>
                  <td class="menu">
                    <a href="http://tomcat.apache.org/">Home Page</a><br/>
    <a href="http://tomcat.apache.org/faq/">FAQ</a><br/>
                    <a href="http://tomcat.apache.org/bugreport.html">Bug D
↪atabase</a><br/>
                    <a href="http://issues.apache.org/bugzilla/buglist.cgi?bug_s
↪tatus=UNCONFIRMED&amp;bug_status=NEW&amp;bug_status=ASSIGNED&amp;bug_status=RE
↪OPENED&amp;bug_status=RESOLVED&amp;resolution=LATER&amp;resolution=REMIND&amp;
↪resolution=---&amp;bugidtype=include&amp;product=Tomcat+5&amp;cmdtype=doit&amp
↪;order=Importance">Open Bugs</a><br/>
                    <a href="http://mail-archives.apache.org/mod_mbox/tomcat-use
↪rs/">Users Mailing List</a><br/>
                    <a href="http://mail-archives.apache.org/mod_mbox/tomcat-dev
↪/">Developers Mailing List</a><br/>
                    <a href="irc://irc.freenode.net/#tomcat">IRC</a><br/>
     
                  </td>
                </tr>
            </table>

            <br/>
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
                  <th>Examples</th>
                </tr>
                <tr>
                  <td class="menu">
                    <a href="jsp-examples/">JSP Examples</a><br/>
                    <a href="servlets-examples/">Servlet Examples</a><br/>
                    <a href="webdav/">WebDAV capabilities</a><br/>
           
                  </td>
                </tr>
            </table>

            <br/>
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
   <th>Miscellaneous</th>
```

... continues on next page ...

. . . continued from previous page . . .

```
                </tr>
                <tr>
                  <td class="menu">
                    <a href="http://java.sun.com/products/jsp">Sun's Java&n
↪bsp;Server Pages Site</a><br/>
                    <a href="http://java.sun.com/products/servlet">Sun's Se
↪rvlet Site</a><br/>
          
                  </td>
                </tr>
            </table>
        </td>
        <td style="width:20px"> </td>

        <!-- Body -->
        <td align="left" valign="top">
          <p id="congrats">If you're seeing this page via a web browser, it mean
↪s you've setup Tomcat successfully. Congratulations!</p>

          <p>As you may have guessed by now, this is the default Tomcat home pag
↪e. It can be found on the local filesystem at:</p>
          <p class="code">$CATALINA_HOME/webapps/ROOT/index.jsp</p>

          <p>where "$CATALINA_HOME" is the root of the Tomcat installation direc
↪tory. If you're seeing this page, and you don't think you should be, then eith
↪er you're either a user who has arrived at new installation of Tomcat, or you'
↪re an administrator who hasn't got his/her setup quite right. Providing the la
↪tter is the case, please refer to the <a href="tomcat-docs">Tomcat Documentati
↪on</a> for more detailed setup and administration information than is found in
↪ the INSTALL file.</p>
            <p><b>NOTE:</b> This page is precompiled. If you change it, this pag
↪e will not change since
                  it was compiled into a servlet at build time.
                  (See <tt>$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml</tt> as t
↪o how it was mapped.)
            </p>
            <p><b>NOTE: For security reasons, using the administration webapp
            is restricted to users with role "admin". The manager webapp
            is restricted to users with role "manager".</b>
            Users are defined in <code>$CATALINA_HOME/conf/tomcat-users.xml</cod
↪e>.</p>
            <p>Included with this release are a host of sample Servlets and JSPs
↪ (with associated source code), extensive documentation (including the Servlet
↪ 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web app
↪lications.</p>
            <p>Tomcat mailing lists are available at the Tomcat project web site
↪:</p>
```

. . . continues on next page . . .

... continued from previous page ...

```
            <ul>
                <li><b><a href="mailto:users@tomcat.apache.org">users@tomc
```

Solution:
Solution type: VendorFix
- Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later
- For other products using Tomcat please contact the vendor for more information on fixed versions

Affected Software/OS
Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled.
Other products like JBoss or Wildfly which are using Tomcat might be affected as well.

Vulnerability Insight
Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code.

Vulnerability Detection Method
Sends a crafted AJP request and checks the response.
Details: `Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.143545
Version used: `2025-07-11T05:42:17Z`

References

```
cve: CVE-2020-1938
url: https://lists.apache.org/thread/bnys5lvg1875dsslkkx2vmwxv833l35x
url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.31
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.51
url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.100
url: https://web.archive.org/web/20250114042903/https://www.chaitin.cn/en/ghostc
↪at
url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487
url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi
url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances
↪-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
cisa: Known Exploited Vulnerability (KEV) catalog
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2023-2480
cert-bund: CB-K20/0711
cert-bund: CB-K20/0705
cert-bund: CB-K20/0693
cert-bund: CB-K20/0555
cert-bund: CB-K20/0543
cert-bund: CB-K20/0154
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-1736
dfn-cert: DFN-CERT-2020-1508
dfn-cert: DFN-CERT-2020-1413
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2020-1134
dfn-cert: DFN-CERT-2020-0850
dfn-cert: DFN-CERT-2020-0835
dfn-cert: DFN-CERT-2020-0821
dfn-cert: DFN-CERT-2020-0569
dfn-cert: DFN-CERT-2020-0557
dfn-cert: DFN-CERT-2020-0501
dfn-cert: DFN-CERT-2020-0381
```

[return to 192.168.56.102]

2.1.9 High 513/tcp

High (CVSS: 10.0)
NVT: rlogin Passwordless Login

Summary
The rlogin service allows root access without a password.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`It was possible to gain root access without a password.`

Impact
This vulnerability allows an attacker to gain complete control over the target system.

Solution:
Solution type: Mitigation
Disable the rlogin service and use alternatives like SSH instead.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `rlogin Passwordless Login`
OID:1.3.6.1.4.1.25623.1.0.113766
Version used: `2020-09-30T09:30:12Z`

[return to 192.168.56.102]

2.1.10 High 8787/tcp

High (CVSS: 10.0)
NVT: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities

Summary
Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
```
The service is running in $SAFE >= 1 mode. However it is still possible to run a
↪rbitrary syscall commands on the remote host. Sending an invalid syscall the s
↪ervice returned the following response:
Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in ‘syscall’"0/usr/lib/
↪ruby/1.8/drb/drb.rb:1555:in ‘send’"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in ‘__se
↪nd__’"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in ‘perform_without_block’"3/usr/lib/
↪ruby/1.8/drb/drb.rb:1515:in ‘perform’"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in ‘m
↪ain_loop’"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in ‘loop’"5/usr/lib/ruby/1.8/drb/
↪drb.rb:1585:in ‘main_loop’"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in ‘start’"5/usr
↪/lib/ruby/1.8/drb/drb.rb:1581:in ‘main_loop’"//usr/lib/ruby/1.8/drb/drb.rb:143
↪0:in ‘run’"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in ‘start’"//usr/lib/ruby/1.8/dr
↪b/drb.rb:1427:in ‘run’"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in ‘initialize’"//us
↪r/lib/ruby/1.8/drb/drb.rb:1627:in ‘new’"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
↪‘start_service’"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
↪plemented
```

Impact
By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.

Solution:
Solution type: Mitigation
Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:
- Implementing taint on untrusted input
- Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate)
- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

Vulnerability Detection Method
Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.
Details: `Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.108010

. . . continues on next page . . .

... continued from previous page ...

Version used: 2024-06-28T05:05:33Z

References
url: https://tools.cisco.com/security/center/viewAlert.x?alertId=22750
url: http://www.securityfocus.com/bid/47071
url: http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_tes
↪ters/
url: http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html

[return to 192.168.56.102]

2.1.11 High 3306/tcp

High (CVSS: 9.8)
NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)

Product detection result
cpe:/a:mysql:mysql:5.0.51a
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)

Summary
It was possible to login into the remote MySQL using default credentials.

Quality of Detection (QoD): 95%

Vulnerability Detection Result
It was possible to login as user "root" with an empty password.

Solution:
Solution type: Mitigation
- Change the password as soon as possible
- Contact the vendor for other possible fixes / updates

Affected Software/OS
The following products are know to use such weak credentials:
- CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x
- CVE-2002-1809: Windows binary release of MySQL 3.23.2 through 3.23.52
- CVE-2004-1532: AppServ 2.5.x and earlier
- CVE-2004-2357: Proofpoint Protection Server
- CVE-2006-1451: MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6
- CVE-2007-2554: Associated Press (AP) Newspower 4.0.1 and earlier
- CVE-2007-6081: AdventNet EventLog Analyzer build 4030
- CVE-2009-0919: XAMPP

... continues on next page ...

... continued from previous page ...

- CVE-2014-3419: Infoblox NetMRI before 6.8.5
- CVE-2015-4669: Xsuite 2.x
- CVE-2016-6531, CVE-2018-15719: Open Dental before version 18.4
- CVE-2024-22901: Vinchin Backup & Recovery 7.2 and prior

Other products might be affected as well.

Vulnerability Detection Method

Details: `MySQL / MariaDB Default Credentials (MySQL Protocol)`
OID:1.3.6.1.4.1.25623.1.0.103551
Version used: `2025-03-14T05:38:04Z`

Product Detection Result

Product: `cpe:/a:mysql:mysql:5.0.51a`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References

`cve: CVE-2001-0645`
`cve: CVE-2002-1809`
`cve: CVE-2004-1532`
`cve: CVE-2004-2357`
`cve: CVE-2006-1451`
`cve: CVE-2007-2554`
`cve: CVE-2007-6081`
`cve: CVE-2009-0919`
`cve: CVE-2014-3419`
`cve: CVE-2015-4669`
`cve: CVE-2016-6531`
`cve: CVE-2018-15719`
`cve: CVE-2024-22901`

[return to 192.168.56.102]