

# Scan Report

January 3, 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 “Report2”. The scan started at Fri Jan 3 15:45:47 2025 UTC and ended at Fri Jan 3 16:19:26 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

<b>1</b>	<b>Result Overview</b>	<b>2</b>
1.1	Host Authentications . . . . .	2
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	10.0.2.5 . . . . .	2
2.1.1	High 512/tcp . . . . .	3
2.1.2	High 80/tcp . . . . .	4
2.1.3	High 8009/tcp . . . . .	8
2.1.4	High 5432/tcp . . . . .	14
2.1.5	High 6697/tcp . . . . .	17
2.1.6	High general/tcp . . . . .	19
2.1.7	High 8787/tcp . . . . .	20
2.1.8	High 3306/tcp . . . . .	21
2.1.9	High 513/tcp . . . . .	23
2.1.10	High 1524/tcp . . . . .	24
2.1.11	High 3632/tcp . . . . .	25
2.1.12	High 514/tcp . . . . .	26
2.1.13	High 2121/tcp . . . . .	27
2.1.14	High 5900/tcp . . . . .	28
2.1.15	High 21/tcp . . . . .	29
2.1.16	High 6200/tcp . . . . .	32
2.1.17	Medium 25/tcp . . . . .	32

2.1.18	Medium 80/tcp . . . . .	50
2.1.19	Medium 5432/tcp . . . . .	64
2.1.20	Medium 23/tcp . . . . .	80
2.1.21	Medium 445/tcp . . . . .	81
2.1.22	Medium 2121/tcp . . . . .	82
2.1.23	Medium 5900/tcp . . . . .	83
2.1.24	Medium 21/tcp . . . . .	83
2.1.25	Medium 22/tcp . . . . .	85
2.1.26	Low 25/tcp . . . . .	89
2.1.27	Low 5432/tcp . . . . .	95
2.1.28	Low general/tcp . . . . .	98
2.1.29	Low 22/tcp . . . . .	99
2.1.30	Low general/icmp . . . . .	101

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
<a href="#">10.0.2.5</a>	22	40	6	0	0
Total: 1	22	40	6	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 68 results selected by the filtering described above. Before filtering there were 605 results.

### 1.1 Host Authentications

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

## 2 Results per Host

### 2.1 10.0.2.5

Host scan start Fri Jan 3 15:46:23 2025 UTC

Host scan end Fri Jan 3 16:19:17 2025 UTC

Service (Port)	Threat Level
<a href="#">512/tcp</a>	High
<a href="#">80/tcp</a>	High
<a href="#">8009/tcp</a>	High
<a href="#">5432/tcp</a>	High
<a href="#">6697/tcp</a>	High
<a href="#">general/tcp</a>	High
<a href="#">8787/tcp</a>	High
<a href="#">3306/tcp</a>	High
<a href="#">513/tcp</a>	High

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
<a href="#">1524/tcp</a>	High
<a href="#">3632/tcp</a>	High
<a href="#">514/tcp</a>	High
<a href="#">2121/tcp</a>	High
<a href="#">5900/tcp</a>	High
<a href="#">21/tcp</a>	High
<a href="#">6200/tcp</a>	High
<a href="#">25/tcp</a>	Medium
<a href="#">80/tcp</a>	Medium
<a href="#">5432/tcp</a>	Medium
<a href="#">23/tcp</a>	Medium
<a href="#">445/tcp</a>	Medium
<a href="#">2121/tcp</a>	Medium
<a href="#">5900/tcp</a>	Medium
<a href="#">21/tcp</a>	Medium
<a href="#">22/tcp</a>	Medium
<a href="#">25/tcp</a>	Low
<a href="#">5432/tcp</a>	Low
<a href="#">general/tcp</a>	Low
<a href="#">22/tcp</a>	Low
<a href="#">general/icmp</a>	Low

### 2.1.1 High 512/tcp

High (CVSS: 10.0)
NVT: The rexec service is running
<b>Summary</b> This remote host is running a rexec service.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The rexec service was detected on the target system.
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the rexec service and use alternatives like SSH instead.
<b>Vulnerability Insight</b> 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. ... continues on next page ...

...continued from previous page ...
The main difference is that rexec authenticates by reading the username and password *unencrypted* from the socket.
<b>Vulnerability Detection Method</b> Checks whether an rexec service is exposed on the target host. Details: <b>The rexec service is running</b> OID:1.3.6.1.4.1.25623.1.0.100111 Version used: 2023-09-12T05:05:19Z
<b>References</b> cve: CVE-1999-0618

[\[ return to 10.0.2.5 \]](#)

### 2.1.2 High 80/tcp

High (CVSS: 10.0)
NVT: TWiki XSS and Command Execution Vulnerabilities
<b>Summary</b> TWiki is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 01.Feb.2003 Fixed version: 4.2.4
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to version 4.2.4 or later.
<b>Affected Software/OS</b> TWiki, TWiki version prior to 4.2.4.
<b>Vulnerability Insight</b> The flaws are due to: - %URLPARAM}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.
... continues on next page ...

...continued from previous page ...
- %SEARCH}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.
<b>Vulnerability Detection Method</b> 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
<b>References</b> 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
<b>Summary</b> PHP is prone to multiple vulnerabilities.
<b>Quality of Detection (QoD): 95%</b>
<b>Vulnerability Detection Result</b> By doing the following HTTP POST request: "HTTP POST" body : <?php phpinfo();?> URL : http://10.0.2.5/cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%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+%63%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>
<b>Impact</b> ... continues on next page ...

...continued from previous page ...
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.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 5.3.13, 5.4.3 or later.
<b>Affected Software/OS</b> PHP versions prior to 5.3.13 and 5.4.x prior to 5.4.3.
<b>Vulnerability Insight</b> 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
<b>Vulnerability Detection Method</b> Send multiple a crafted HTTP POST requests and checks the responses. This script checks for the presence of CVE-2012-1823 which indicates that the system is also vulnerable against 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: 2024-11-26T07:35:52Z
<b>References</b> 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/new-s/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
... continues on next page ...

...continued from previous page ...

```
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: 7.5)

NVT: Test HTTP dangerous methods

**Summary**

Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.

**Quality of Detection (QoD): 99%****Vulnerability Detection Result**

We could upload the following files via the PUT method at this web server:

<http://10.0.2.5/dav/puttest1585660532.html>

We could delete the following files via the DELETE method at this web server:

<http://10.0.2.5/dav/puttest1585660532.html>

**Impact**

- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.

- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

**Solution:**

**Solution type:** Mitigation

Use access restrictions to these dangerous HTTP methods or disable them completely.

... continues on next page ...



...continued from previous page ...
<b>Affected Software/OS</b> Web servers with enabled PUT and/or DELETE methods.
<b>Vulnerability Detection Method</b> Checks if dangerous HTTP methods such as PUT and DELETE are enabled and can be misused to upload or delete files. Details: Test HTTP dangerous methods OID:1.3.6.1.4.1.25623.1.0.10498 Version used: 2023-08-01T13:29:10Z
<b>References</b> url: <a href="http://www.securityfocus.com/bid/12141">http://www.securityfocus.com/bid/12141</a> owasp: OWASP-CM-001

[\[ return to 10.0.2.5 \]](#)

### 2.1.3 High 8009/tcp

High (CVSS: 9.8) NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)
<b>Summary</b> Apache Tomcat is prone to a remote code execution (RCE) vulnerability (dubbed 'Ghostcat') in the AJP connector.
<b>Quality of Detection (QoD): 99%</b>
<b>Vulnerability Detection Result</b> It was possible to read the file "/WEB-INF/web.xml" through the AJP connector. Result: AB 8\x0004 Ã\x0088 \x00020K \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 <a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a> 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.
...continues on next page ...

...continued from previous page...

```
-->
<?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">
      /**/
        body {
          color: #000000;
          background-color: #FFFFFF;
          font-family: Arial, "Times New Roman", Times, serif;
          margin: 10px 0px;
        }
        img {
          border: none;
        }

        a:link, a:visited {
          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;
        }
      ]]]&gt;
    </pre>
</div>
<div data-bbox="155 799 377 814" data-label="Text">...continues on next page...</div>
```

...continued from previous page ...

```

#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>
        <td align="left" style="width:130px">
            <a href="http://tomcat.apache.org/">
                />
            </a>
        </td>
        <td align="left" valign="top"><b>Apache Tomcat/5.5</b></td>
        <td align="right">
            <a href="http://www.apache.org/">
                
            </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&nbsp; Administration</a><br/>

```

...continues on next page ...

...continued from previous page ...	
	<pre> &lt;a href="manager/html"&gt;Tomcat&amp;nbsp;Manager&lt;/a&gt;&lt;br/&gt; &amp;nbsp; &lt;/td&gt; &lt;/tr&gt; &lt;/table&gt; &lt;br /&gt; &lt;table width="100%" border="1" cellspacing="0" cellpadding="3"&gt;   &lt;tr&gt; &lt;th&gt;Documentation&lt;/th&gt;     &lt;tr&gt;       &lt;tr&gt;         &lt;td class="menu"&gt;           &lt;a href="RELEASE-NOTES.txt"&gt;Release&amp;nbsp;Notes&lt;/a&gt;&lt;br/&gt;           &lt;a href="tomcat-docs/changelog.html"&gt;Change&amp;nbsp;Log&lt;/a&gt;&lt;br/&gt; ↪&gt;           &lt;a href="tomcat-docs"&gt;Tomcat&amp;nbsp;Documentation&lt;/a&gt;&lt;br/&gt; ↪           &amp;nbsp;           &amp;nbsp;         &lt;/td&gt;       &lt;/tr&gt;     &lt;/table&gt;  &lt;br/&gt; &lt;table width="100%" border="1" cellspacing="0" cellpadding="3"&gt;   &lt;tr&gt;     &lt;th&gt;Tomcat Online&lt;/th&gt;   &lt;/tr&gt;   &lt;tr&gt;     &lt;td class="menu"&gt;       &lt;a href="http://tomcat.apache.org/"&gt;Home&amp;nbsp;Page&lt;/a&gt;&lt;br/&gt;       &lt;a href="http://tomcat.apache.org/faq/"&gt;FAQ&lt;/a&gt;&lt;br/&gt;       &lt;a href="http://tomcat.apache.org/bugreport.html"&gt;Bug&amp;nbsp;D ↪atabase&lt;/a&gt;&lt;br/&gt;       &lt;a href="http://issues.apache.org/bugzilla/buglist.cgi?bug_s ↪tatus=UNCONFIRMED&amp;amp;bug_status=NEW&amp;amp;bug_status=ASSIGNED&amp;amp;bug_status=RE ↪OPENED&amp;amp;bug_status=RESOLVED&amp;amp;resolution=LATER&amp;amp;resolution=REMIND&amp;amp; ↪resolution=---&amp;amp;bugidtype=include&amp;amp;product=Tomcat+5&amp;amp;cmdtype=doit&amp;amp ↪;order=Importance"&gt;Open Bugs&lt;/a&gt;&lt;br/&gt;       &lt;a href="http://mail-archives.apache.org/mod_mbox/tomcat-use ↪rs/"&gt;Users&amp;nbsp;Mailing&amp;nbsp;List&lt;/a&gt;&lt;br/&gt;       &lt;a href="http://mail-archives.apache.org/mod_mbox/tomcat-dev ↪/"&gt;Developers&amp;nbsp;Mailing&amp;nbsp;List&lt;/a&gt;&lt;br/&gt;       &lt;a href="irc://irc.freenode.net/#tomcat"&gt;IRC&lt;/a&gt;&lt;br/&gt;       &amp;nbsp;     &lt;/td&gt;   &lt;/tr&gt; &lt;/table&gt; </pre>
... continues on next page ...	

...continued from previous page...

```

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

<br/>
<table width="100%" border="1" cellspacing="0" cellpadding="3">
  <tr>
    <th>Miscellaneous</th>
  </tr>
  <tr>
    <td class="menu">
      <a href="http://java.sun.com/products/jsp">Sun's&nbsp;Java&
↳bsp;Server&nbsp;Pages&nbsp;Site</a><br/>
      <a href="http://java.sun.com/products/servlet">Sun's&nbsp;Se
↳rvlet&nbsp;Site</a><br/>
&nbsp;
    </td>
  </tr>
</table>
</td>
<td style="width:20px">&nbsp;</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
...continues on next page ...

```

<div>...continued from previous page ...</div> <div><div>⇐t</div><div>ter is the case, please refer to the &lt;a href="tomcat-docs"&gt;Tomcat Documentati</div><div>⇐on&lt;/a&gt; for more detailed setup and administration information than is found in</div><div>⇐ the INSTALL file.&lt;/p&gt;</div><div><div>&lt;p&gt;&lt;b&gt;NOTE:&lt;/b&gt; This page is precompiled. If you change it, this pag</div><div>⇐e will not change since</div><div>it was compiled into a servlet at build time.</div><div>(See &lt;tt&gt;\$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml&lt;/tt&gt; as t</div><div>⇐o how it was mapped.)</div><div>&lt;/p&gt;</div><div><div>&lt;p&gt;&lt;b&gt;NOTE: For security reasons, using the administration webapp</div><div>is restricted to users with role "admin". The manager webapp</div><div>is restricted to users with role "manager".&lt;/b&gt;</div><div>Users are defined in &lt;code&gt;\$CATALINA_HOME/conf/tomcat-users.xml&lt;/cod</div><div>⇐e&gt;.&lt;/p&gt;</div><div><div>&lt;p&gt;Included with this release are a host of sample Servlets and JSPs</div><div>⇐ (with associated source code), extensive documentation (including the Servlet</div><div>⇐ 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web app</div><div>⇐lications.&lt;/p&gt;</div><div><div>&lt;p&gt;Tomcat mailing lists are available at the Tomcat project web site</div><div>⇐:&lt;/p&gt;</div><div>&lt;ul&gt;</div><div><div>&lt;li&gt;&lt;b&gt;&lt;a href="mailto:users@tomcat.apache.org"&gt;users@tomc</div></div></div></div></div></div></div>
<div><b>Solution:</b></div> <div><b>Solution type:</b> VendorFix</div> <div>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.</div>
<div><b>Affected Software/OS</b></div> <div>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.</div>
<div><b>Vulnerability Insight</b></div> <div>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.</div>
<div><b>Vulnerability Detection Method</b></div> <div>Sends a crafted AJP request and checks the response.</div> <div>Details: Apache Tomcat AJP RCE Vulnerability (Ghostcat)</div> <div>OID:1.3.6.1.4.1.25623.1.0.143545</div> <div>Version used: 2024-06-28T15:38:46Z</div>
<div><b>References</b></div> <div>cve: CVE-2020-1938</div> <div>cisa: Known Exploited Vulnerability (KEV) catalog</div>
<div>... continues on next page ...</div>

...continued from previous page...
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1↪a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E
url: https://www.chaitin.cn/en/ghostcat
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://tomcat.apache.org/tomcat-7.0-doc/changelog.html
url: https://tomcat.apache.org/tomcat-8.5-doc/changelog.html
url: https://tomcat.apache.org/tomcat-9.0-doc/changelog.html
cert-bund: WID-SEC-2023-2480
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

[\[ return to 10.0.2.5 \]](#)

#### 2.1.4 High 5432/tcp

High (CVSS: 9.0)
NVT: PostgreSQL Default Credentials (PostgreSQL Protocol)
<b>Product detection result</b> cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.12802↪5)
<b>Summary</b> It was possible to login into the remote PostgreSQL as user postgres using weak credentials.
<b>Quality of Detection (QoD): 99%</b>
<b>Vulnerability Detection Result</b>
... continues on next page ...

...continued from previous page ...
It was possible to login as user postgres with password "postgres".
<b>Solution:</b> <b>Solution type:</b> Mitigation Change the password as soon as possible.
<b>Vulnerability Detection Method</b> Details: PostgreSQL Default Credentials (PostgreSQL Protocol) OID:1.3.6.1.4.1.25623.1.0.103552 Version used: 2024-07-19T15:39:06Z
<b>Product Detection Result</b> Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.128025)

High (CVSS: 7.4)
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
<b>Summary</b> OpenSSL is prone to security-bypass vulnerability.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.
<b>Vulnerability Insight</b> ... continues on next page ...



...continued from previous page ...
<p>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.</p>
<p><b>Vulnerability Detection Method</b>  Send two SSL ChangeCipherSpec request and check the response.  Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability  OID:1.3.6.1.4.1.25623.1.0.105042  Version used: 2024-09-27T05:05:23Z</p>
<p><b>References</b>  cve: CVE-2014-0224  url: <a href="https://www.openssl.org/news/secadv/20140605.txt">https://www.openssl.org/news/secadv/20140605.txt</a>  url: <a href="http://www.securityfocus.com/bid/67899">http://www.securityfocus.com/bid/67899</a>  cert-bund: WID-SEC-2023-0500  cert-bund: CB-K15/0567  cert-bund: CB-K15/0415  cert-bund: CB-K15/0384  cert-bund: CB-K15/0080  cert-bund: CB-K15/0079  cert-bund: CB-K15/0074  cert-bund: CB-K14/1617  cert-bund: CB-K14/1537  cert-bund: CB-K14/1299  cert-bund: CB-K14/1297  cert-bund: CB-K14/1294  cert-bund: CB-K14/1202  cert-bund: CB-K14/1174  cert-bund: CB-K14/1153  cert-bund: CB-K14/0876  cert-bund: CB-K14/0756  cert-bund: CB-K14/0746  cert-bund: CB-K14/0736  cert-bund: CB-K14/0722  cert-bund: CB-K14/0716  cert-bund: CB-K14/0708  cert-bund: CB-K14/0684  cert-bund: CB-K14/0683  cert-bund: CB-K14/0680  dfn-cert: DFN-CERT-2016-0388  dfn-cert: DFN-CERT-2015-0593  dfn-cert: DFN-CERT-2015-0427  dfn-cert: DFN-CERT-2015-0396  dfn-cert: DFN-CERT-2015-0082  dfn-cert: DFN-CERT-2015-0079  dfn-cert: DFN-CERT-2015-0078</p>
...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1364
dfn-cert: DFN-CERT-2014-1357
dfn-cert: DFN-CERT-2014-1350
dfn-cert: DFN-CERT-2014-1265
dfn-cert: DFN-CERT-2014-1209
dfn-cert: DFN-CERT-2014-0917
dfn-cert: DFN-CERT-2014-0789
dfn-cert: DFN-CERT-2014-0778
dfn-cert: DFN-CERT-2014-0768
dfn-cert: DFN-CERT-2014-0752
dfn-cert: DFN-CERT-2014-0747
dfn-cert: DFN-CERT-2014-0738
dfn-cert: DFN-CERT-2014-0715
dfn-cert: DFN-CERT-2014-0714
dfn-cert: DFN-CERT-2014-0709
```

[\[ return to 10.0.2.5 \]](#)**2.1.5 High 6697/tcp****High (CVSS: 8.1)****NVT: UnrealIRCd Authentication Spoofing Vulnerability****Product detection result**

cpe:/a:unrealircd:unrealircd:3.2.8.1

Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)

**Summary**

UnrealIRCd is prone to authentication spoofing vulnerability.

**Quality of Detection (QoD): 80%****Vulnerability Detection Result**

Installed version: 3.2.8.1

Fixed version: 3.2.10.7

**Impact**

Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.

**Solution:**

... continues on next page ...

...continued from previous page ...
<b>Solution type:</b> VendorFix Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.
<b>Affected Software/OS</b> UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.
<b>Vulnerability Insight</b> The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: UnrealIRCd Authentication Spoofing Vulnerability OID:1.3.6.1.4.1.25623.1.0.809883 Version used: 2023-07-14T16:09:27Z
<b>Product Detection Result</b> Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection OID: 1.3.6.1.4.1.25623.1.0.809884)
<b>References</b> cve: CVE-2016-7144 url: <a href="http://seclists.org/oss-sec/2016/q3/420">http://seclists.org/oss-sec/2016/q3/420</a> url: <a href="http://www.securityfocus.com/bid/92763">http://www.securityfocus.com/bid/92763</a> url: <a href="http://www.openwall.com/lists/oss-security/2016/09/05/8">http://www.openwall.com/lists/oss-security/2016/09/05/8</a> url: <a href="https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b">https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b</a> ↪c50ba1a34a766 url: <a href="https://bugs.unrealircd.org/main_page.php">https://bugs.unrealircd.org/main_page.php</a>

High (CVSS: 7.5)

NVT: UnrealIRCd Backdoor

#### Summary

Detection of backdoor in UnrealIRCd.

**Quality of Detection (QoD):** 70%

#### Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

#### Solution:

**Solution type:** VendorFix

Install latest version of unrealircd and check signatures of software you're installing.

... continues on next page ...

...continued from previous page ...
<p><b>Affected Software/OS</b></p> <p>The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.</p>
<p><b>Vulnerability Insight</b></p> <p>Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Details: UnrealIRCd Backdoor  OID:1.3.6.1.4.1.25623.1.0.80111  Version used: 2023-08-01T13:29:10Z</p>
<p><b>References</b></p> <p>cve: CVE-2010-2075  url: <a href="http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt">http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt</a>  url: <a href="http://seclists.org/fulldisclosure/2010/Jun/277">http://seclists.org/fulldisclosure/2010/Jun/277</a>  url: <a href="http://www.securityfocus.com/bid/40820">http://www.securityfocus.com/bid/40820</a></p>

[\[ return to 10.0.2.5 \]](#)

### 2.1.6 High general/tcp

<p>High (CVSS: 10.0)</p> <p>NVT: Operating System (OS) End of Life (EOL) Detection</p>
<p><b>Product detection result</b></p> <p>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)</p>
<p><b>Summary</b></p> <p>The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.</p>
<p><b>Quality of Detection (QoD): 80%</b></p>
<p><b>Vulnerability Detection Result</b></p> <p>The "Ubuntu" Operating System on the remote host has reached the end of life.</p>
... continues on next page ...

...continued from previous page ...	
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
<b>Impact</b> 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.	
<b>Solution:</b> <b>Solution type:</b> Mitigation Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.	
<b>Vulnerability Detection Method</b> Checks if an EOL version of an OS is present on the target host. Details: Operating System (OS) End of Life (EOL) Detection OID:1.3.6.1.4.1.25623.1.0.103674 Version used: 2024-02-28T14:37:42Z	
<b>Product Detection Result</b> 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)	

[\[ return to 10.0.2.5 \]](#)

2.1.7 High 8787/tcp

High (CVSS: 10.0)
NVT: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities
<b>Summary</b> Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> The service is running in \$SAFE >= 1 mode. However it is still possible to run a ↵rbbitrary syscall commands on the remote host. Sending an invalid syscall the s ↵ervice returned the following response:
... continues on next page ...

<div>...continued from previous page...</div> <div>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</div>
<div><b>Impact</b></div> <div>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.</div>
<div><b>Solution:</b></div> <div><b>Solution type:</b> Mitigation</div> <div>Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:</div> <div><ul style="list-style-type: none"><li>- Implementing taint on untrusted input</li><li>- Setting \$SAFE levels appropriately (&gt;=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and &gt;=3 may be appropriate)</li><li>- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts</li></ul></div>
<div><b>Vulnerability Detection Method</b></div> <div>Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.</div> <div>Details: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities</div> <div>OID:1.3.6.1.4.1.25623.1.0.108010</div> <div>Version used: 2024-06-28T05:05:33Z</div>
<div><b>References</b></div> <div>url: <a href="https://tools.cisco.com/security/center/viewAlert.x?alertId=22750">https://tools.cisco.com/security/center/viewAlert.x?alertId=22750</a></div> <div>url: <a href="http://www.securityfocus.com/bid/47071">http://www.securityfocus.com/bid/47071</a></div> <div>url: <a href="http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testing/">http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testing/</a></div> <div>url: <a href="http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html">http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html</a></div>

[\[ return to 10.0.2.5 \]](#)

2.1.8 High 3306/tcp

<p>High (CVSS: 9.8)</p> <p>NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)</p>
<p><b>Product detection result</b></p> <p>cpe:/a:mysql:mysql:5.0.51a</p> <p>Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.↵25623.1.0.100152)</p>
<p><b>Summary</b></p> <p>It was possible to login into the remote MySQL as root using weak credentials.</p>
<p><b>Quality of Detection (QoD): 95%</b></p>
<p><b>Vulnerability Detection Result</b></p> <p>It was possible to login as root with an empty password.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <ul style="list-style-type: none"> <li>- Change the password as soon as possible</li> <li>- Contact the vendor for other possible fixes / updates</li> </ul>
<p><b>Affected Software/OS</b></p> <p>The following products are know to use such weak credentials:</p> <ul style="list-style-type: none"> <li>- CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x</li> <li>- CVE-2004-2357: Proofpoint Protection Server</li> <li>- CVE-2006-1451: MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6</li> <li>- CVE-2007-2554: Associated Press (AP) Newspower 4.0.1 and earlier</li> <li>- CVE-2007-6081: AdventNet EventLog Analyzer build 4030</li> <li>- CVE-2009-0919: XAMPP</li> <li>- CVE-2014-3419: Infoblox NetMRI before 6.8.5</li> <li>- CVE-2015-4669: Xsuite 2.x</li> <li>- CVE-2016-6531, CVE-2018-15719: Open Dental before version 18.4</li> </ul> <p>Other products might be affected as well.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Details: MySQL / MariaDB Default Credentials (MySQL Protocol)</p> <p>OID:1.3.6.1.4.1.25623.1.0.103551</p> <p>Version used: 2023-11-02T05:05:26Z</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:mysql:mysql:5.0.51a</p> <p>Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>... continues on next page ...</p>

...continued from previous page ...

**References**

cve: CVE-2001-0645  
 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

[\[ return to 10.0.2.5 \]](#)**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



High (CVSS: 7.5)
NVT: The rlogin service is running
<b>Summary</b> This remote host is running a rlogin service.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The rlogin service is running on the target system.
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the rlogin service and use alternatives like SSH instead.
<b>Vulnerability Insight</b> rlogin has several serious security problems, - all information, including passwords, is transmitted unencrypted. - .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password)
<b>Vulnerability Detection Method</b> Details: The rlogin service is running OID:1.3.6.1.4.1.25623.1.0.901202 Version used: 2021-09-01T07:45:06Z
<b>References</b> cve: CVE-1999-0651

[\[ return to 10.0.2.5 \]](#)

#### 2.1.10 High 1524/tcp

High (CVSS: 10.0)
NVT: Possible Backdoor: Ingreslock
<b>Summary</b> A backdoor is installed on the remote host.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> The service is answering to an 'id;' command with the following response: uid=0( ... continues on next page ...

...continued from previous page ...
↔root) gid=0(root)
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.
<b>Solution:</b> <b>Solution type:</b> Workaround A whole cleanup of the infected system is recommended.
<b>Vulnerability Detection Method</b> Details: Possible Backdoor: Ingreslock OID:1.3.6.1.4.1.25623.1.0.103549 Version used: 2023-07-25T05:05:58Z

[\[ return to 10.0.2.5 \]](#)

### 2.1.11 High 3632/tcp

High (CVSS: 9.3)
NVT: DistCC RCE Vulnerability (CVE-2004-2687)
<b>Summary</b> DistCC is prone to a remote code execution (RCE) vulnerability.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> It was possible to execute the "id" command. Result: uid=1(daemon) gid=1(daemon)
<b>Impact</b> DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.
<b>Solution:</b> <b>Solution type:</b> VendorFix Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references.
<b>Vulnerability Insight</b>
... continues on next page ...

...continued from previous page ...
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.
<b>Vulnerability Detection Method</b> 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
<b>References</b> cve: CVE-2004-2687 url: <a href="https://distcc.github.io/security.html">https://distcc.github.io/security.html</a> url: <a href="https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80">https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80</a> ↪/archives/bugtraq/2005-03/0183.html dfn-cert: DFN-CERT-2019-0381

[\[ return to 10.0.2.5 \]](#)

### 2.1.12 High 514/tcp

<b>High (CVSS: 7.5)</b> <b>NVT: rsh Unencrypted Cleartext Login</b>
<b>Summary</b> This remote host is running a rsh service.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> The rsh service is misconfigured so it is allowing connections without a password ↪d or with default root:root credentials.
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the rsh service and use alternatives like SSH instead.
<b>Vulnerability Insight</b> rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network. Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.
... continues on next page ...

...continued from previous page ...
<b>Vulnerability Detection Method</b> Details: rsh Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.100080 Version used: 2021-10-20T09:03:29Z
<b>References</b> cve: CVE-1999-0651

[\[ return to 10.0.2.5 \]](#)

### 2.1.13 High 2121/tcp

High (CVSS: 7.5) NVT: FTP Brute Force Logins Reporting
<b>Summary</b> It was possible to login into the remote FTP server using weak/known credentials.
<b>Quality of Detection (QoD):</b> 95%
<b>Vulnerability Detection Result</b> It was possible to login with the following credentials <User>:<Password> msfadmin:msfadmin postgres:postgres service:service user:user
<b>Impact</b> This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.
<b>Solution:</b> <b>Solution type:</b> Mitigation Change the password as soon as possible.
<b>Vulnerability Insight</b> The following devices are / software is known to be affected: <ul style="list-style-type: none"> <li>- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&amp;R</li> <li>- CVE-2013-7404: GE Healthcare Discovery NM 750b</li> <li>- CVE-2014-9198: Schneider Electric ETG3000 FactoryCast HMI gateways</li> <li>- CVE-2015-7261: QNAP iArtist Lite distributed with QNAP Signage Station</li> <li>- CVE-2016-8731: Foscam C1 devices</li> <li>- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices</li> </ul>
... continues on next page ...

...continued from previous page ...
<div>- CVE-2018-9068: IMM2 for IBM and Lenovo System x</div> <div>- CVE-2018-17771: Ingenico Telium 2 PoS terminals</div> <div>- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices</div> <div>Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.</div>
<div><b>Vulnerability Detection Method</b></div> <div>Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).</div> <div>Details: FTP Brute Force Logins Reporting</div> <div>OID:1.3.6.1.4.1.25623.1.0.108718</div> <div>Version used: 2024-12-17T05:05:41Z</div>
<div><b>References</b></div> <div>cve: CVE-1999-0501</div> <div>cve: CVE-1999-0502</div> <div>cve: CVE-1999-0507</div> <div>cve: CVE-1999-0508</div> <div>cve: CVE-2001-1594</div> <div>cve: CVE-2013-7404</div> <div>cve: CVE-2014-9198</div> <div>cve: CVE-2015-7261</div> <div>cve: CVE-2016-8731</div> <div>cve: CVE-2017-8218</div> <div>cve: CVE-2018-9068</div> <div>cve: CVE-2018-17771</div> <div>cve: CVE-2018-19063</div> <div>cve: CVE-2018-19064</div>

[\[ return to 10.0.2.5 \]](#)

2.1.14 High 5900/tcp

<div>High (CVSS: 9.0)</div> <div>NVT: VNC Brute Force Login</div>
<div><b>Summary</b></div> <div>Try to log in with given passwords via VNC protocol.</div>
<div><b>Quality of Detection (QoD):</b> 95%</div>
<div><b>Vulnerability Detection Result</b></div> <div>It was possible to connect to the VNC server with the password: password</div>
...continues on next page ...

...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> Mitigation Change the password to something hard to guess or enable password protection at all.
<b>Vulnerability Insight</b> This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all. Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked. Note as well that passwords can be max. 8 characters long.
<b>Vulnerability Detection Method</b> Details: VNC Brute Force Login OID:1.3.6.1.4.1.25623.1.0.106056 Version used: 2021-07-23T07:56:26Z

[\[ return to 10.0.2.5 \]](#)

### 2.1.15 High 21/tcp

High (CVSS: 9.8)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability
<b>Product detection result</b> cpe:/a:beasts:vsftpd:2.3.4 Detected by vsFTPD FTP Server Detection (OID: 1.3.6.1.4.1.25623.1.0.111050)
<b>Summary</b> vsftpd is prone to a backdoor vulnerability.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
<b>Solution:</b> <b>Solution type:</b> VendorFix
... continues on next page ...

...continued from previous page ...
The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.
<b>Affected Software/OS</b> The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.
<b>Vulnerability Insight</b> The tainted source package contains a backdoor which opens a shell on port 6200/tcp.
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> Product: cpe:/a:beasts:vsftpd:2.3.4 Method: vsFTPd FTP Server Detection OID: 1.3.6.1.4.1.25623.1.0.111050)
<b>References</b> cve: CVE-2011-2523 url: <a href="https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html">https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html</a> url: <a href="https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bid/48539/">https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bid/48539/</a> url: <a href="https://security.appspot.com/vsftpd.html">https://security.appspot.com/vsftpd.html</a>

High (CVSS: 7.5)
NVT: FTP Brute Force Logins Reporting
<b>Summary</b> It was possible to login into the remote FTP server using weak/known credentials.
<b>Quality of Detection (QoD):</b> 95%
<b>Vulnerability Detection Result</b> It was possible to login with the following credentials <User>:<Password> msfadmin:msfadmin postgres:postgres service:service user:user
<b>Impact</b> ... continues on next page ...

...continued from previous page ...
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.
<b>Solution:</b> <b>Solution type:</b> Mitigation Change the password as soon as possible.
<b>Vulnerability Insight</b> The following devices are / software is known to be affected: - CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R - CVE-2013-7404: GE Healthcare Discovery NM 750b - CVE-2014-9198: Schneider Electric ETG3000 FactoryCast HMI gateways - CVE-2015-7261: QNAP iArtist Lite distributed with QNAP Signage Station - CVE-2016-8731: Foscam C1 devices - CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices - CVE-2018-9068: IMM2 for IBM and Lenovo System x - CVE-2018-17771: Ingenico Telium 2 PoS terminals - CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.
<b>Vulnerability Detection Method</b> Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717). Details: FTP Brute Force Logins Reporting OID:1.3.6.1.4.1.25623.1.0.108718 Version used: 2024-12-17T05:05:41Z
<b>References</b> cve: CVE-1999-0501 cve: CVE-1999-0502 cve: CVE-1999-0507 cve: CVE-1999-0508 cve: CVE-2001-1594 cve: CVE-2013-7404 cve: CVE-2014-9198 cve: CVE-2015-7261 cve: CVE-2016-8731 cve: CVE-2017-8218 cve: CVE-2018-9068 cve: CVE-2018-17771 cve: CVE-2018-19063 cve: CVE-2018-19064



**2.1.16 High 6200/tcp**

High (CVSS: 9.8)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability
<b>Summary</b> vsftpd is prone to a backdoor vulnerability.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
<b>Solution:</b> <b>Solution type:</b> VendorFix The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.
<b>Affected Software/OS</b> The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.
<b>Vulnerability Insight</b> The tainted source package contains a backdoor which opens a shell on port 6200/tcp.
<b>Vulnerability Detection Method</b> 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
<b>References</b> cve: CVE-2011-2523 url: <a href="https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html">https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html</a> url: <a href="https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bid/48539/">https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bid/48539/</a> url: <a href="https://security.appspot.com/vsftpd.html">https://security.appspot.com/vsftpd.html</a>

[\[ return to 10.0.2.5 \]](#)

**2.1.17 Medium 25/tcp**

Medium (CVSS: 6.8)
NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability
<b>Summary</b> Multiple vendors' implementations of 'STARTTLS' are prone to a vulnerability that lets attackers inject arbitrary commands.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> An attacker can exploit this issue to execute arbitrary commands in the context of the user running the application. Successful exploits can allow attackers to obtain email usernames and passwords.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> The following vendors are known to be affected: Ipswitch Kerio Postfix Qmail-TLS Oracle SCO Group spamdyke ISC
<b>Vulnerability Detection Method</b> Send a special crafted 'STARTTLS' request and check the response. Details: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection . ↪.. OID:1.3.6.1.4.1.25623.1.0.103935 Version used: 2023-10-31T05:06:37Z
<b>References</b> cve: CVE-2011-0411 cve: CVE-2011-1430 cve: CVE-2011-1431 cve: CVE-2011-1432 ... continues on next page ...

...continued from previous page...

cve: CVE-2011-1506  
cve: CVE-2011-1575  
cve: CVE-2011-1926  
cve: CVE-2011-2165  
url: <http://www.securityfocus.com/bid/46767>  
url: <http://kolab.org/pipermail/kolab-announce/2011/000101.html>  
url: [http://bugzilla.cyrusimap.org/show\\_bug.cgi?id=3424](http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424)  
url: [http://cyrusimap.org/mediawiki/index.php/Bugs\\_Resolved\\_in\\_2.4.7](http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7)  
url: <http://www.kb.cert.org/vuls/id/MAPG-8D9M4P>  
url: [http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-no  
↔tes.txt](http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-notes.tes.txt)  
url: <http://www.postfix.org/CVE-2011-0411.html>  
url: <http://www.pureftpd.org/project/pure-ftpd/news>  
url: [http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN\\_ReleaseNotes  
↔XCS\\_9\\_1\\_1/EN\\_ReleaseNotes\\_WG\\_XCS\\_9\\_1\\_TLS\\_Hotfix.pdf](http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_↔XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf)  
url: <http://www.spamdyke.org/documentation/Changelog.txt>  
url: [http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include  
↔\\_text=1](http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include_↔_text=1)  
url: <http://www.securityfocus.com/archive/1/516901>  
url: <http://support.avaya.com/css/P8/documents/100134676>  
url: <http://support.avaya.com/css/P8/documents/100141041>  
url: <http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>  
url: <http://inco.net/qmail-tls/vu555316.patch>  
url: <http://www.kb.cert.org/vuls/id/555316>  
cert-bund: CB-K15/1514  
dfn-cert: DFN-CERT-2011-0917  
dfn-cert: DFN-CERT-2011-0912  
dfn-cert: DFN-CERT-2011-0897  
dfn-cert: DFN-CERT-2011-0844  
dfn-cert: DFN-CERT-2011-0818  
dfn-cert: DFN-CERT-2011-0808  
dfn-cert: DFN-CERT-2011-0771  
dfn-cert: DFN-CERT-2011-0741  
dfn-cert: DFN-CERT-2011-0712  
dfn-cert: DFN-CERT-2011-0673  
dfn-cert: DFN-CERT-2011-0597  
dfn-cert: DFN-CERT-2011-0596  
dfn-cert: DFN-CERT-2011-0519  
dfn-cert: DFN-CERT-2011-0516  
dfn-cert: DFN-CERT-2011-0483  
dfn-cert: DFN-CERT-2011-0434  
dfn-cert: DFN-CERT-2011-0393  
dfn-cert: DFN-CERT-2011-0381

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
<b>Product detection result</b> cpe:/a:ietf:transport_layer_security:1.0 Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
<b>Summary</b> It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and S ↪SSLv3 protocols and supports one or more ciphers. Those supported ciphers can b ↪e found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256 ↪23.1.0.802067) VT.
<b>Impact</b> An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
<b>Solution:</b> <b>Solution type:</b> Mitigation It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
<b>Affected Software/OS</b> All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
<b>Vulnerability Insight</b> The SSLv2 and SSLv3 protocols contain known cryptographic flaws like: - CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE) - CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)
<b>Vulnerability Detection Method</b> Check the used SSL protocols of the services provided by this system. Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012 Version used: 2024-09-27T05:05:23Z
... continues on next page ...

...continued from previous page ...

**Product Detection Result**

Product: cpe:/a:ietf:transport\_layer\_security:1.0

Method: SSL/TLS: Version Detection

OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2016-0800

cve: CVE-2014-3566

url: <https://ssl-config.mozilla.org/>url: <https://bettercrypto.org/>url: <https://drownattack.com/>url: <https://www.imperialviolet.org/2014/10/14/poodle.html>url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters>

↔-report-2014

cert-bund: WID-SEC-2023-0431

cert-bund: WID-SEC-2023-0427

cert-bund: CB-K18/0094

cert-bund: CB-K17/1198

cert-bund: CB-K17/1196

cert-bund: CB-K16/1828

cert-bund: CB-K16/1438

cert-bund: CB-K16/1384

cert-bund: CB-K16/1141

cert-bund: CB-K16/1107

cert-bund: CB-K16/1102

cert-bund: CB-K16/0792

cert-bund: CB-K16/0599

cert-bund: CB-K16/0597

cert-bund: CB-K16/0459

cert-bund: CB-K16/0456

cert-bund: CB-K16/0433

cert-bund: CB-K16/0424

cert-bund: CB-K16/0415

cert-bund: CB-K16/0413

cert-bund: CB-K16/0374

cert-bund: CB-K16/0367

cert-bund: CB-K16/0331

cert-bund: CB-K16/0329

cert-bund: CB-K16/0328

cert-bund: CB-K16/0156

cert-bund: CB-K15/1514

cert-bund: CB-K15/1358

cert-bund: CB-K15/1021

cert-bund: CB-K15/0972

cert-bund: CB-K15/0637

... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0590  
 cert-bund: CB-K15/0525  
 cert-bund: CB-K15/0393  
 cert-bund: CB-K15/0384  
 cert-bund: CB-K15/0287  
 cert-bund: CB-K15/0252  
 cert-bund: CB-K15/0246  
 cert-bund: CB-K15/0237  
 cert-bund: CB-K15/0118  
 cert-bund: CB-K15/0110  
 cert-bund: CB-K15/0108  
 cert-bund: CB-K15/0080  
 cert-bund: CB-K15/0078  
 cert-bund: CB-K15/0077  
 cert-bund: CB-K15/0075  
 cert-bund: CB-K14/1617  
 cert-bund: CB-K14/1581  
 cert-bund: CB-K14/1537  
 cert-bund: CB-K14/1479  
 cert-bund: CB-K14/1458  
 cert-bund: CB-K14/1342  
 cert-bund: CB-K14/1314  
 cert-bund: CB-K14/1313  
 cert-bund: CB-K14/1311  
 cert-bund: CB-K14/1304  
 cert-bund: CB-K14/1296  
 dfn-cert: DFN-CERT-2018-0096  
 dfn-cert: DFN-CERT-2017-1238  
 dfn-cert: DFN-CERT-2017-1236  
 dfn-cert: DFN-CERT-2016-1929  
 dfn-cert: DFN-CERT-2016-1527  
 dfn-cert: DFN-CERT-2016-1468  
 dfn-cert: DFN-CERT-2016-1216  
 dfn-cert: DFN-CERT-2016-1174  
 dfn-cert: DFN-CERT-2016-1168  
 dfn-cert: DFN-CERT-2016-0884  
 dfn-cert: DFN-CERT-2016-0841  
 dfn-cert: DFN-CERT-2016-0644  
 dfn-cert: DFN-CERT-2016-0642  
 dfn-cert: DFN-CERT-2016-0496  
 dfn-cert: DFN-CERT-2016-0495  
 dfn-cert: DFN-CERT-2016-0465  
 dfn-cert: DFN-CERT-2016-0459  
 dfn-cert: DFN-CERT-2016-0453  
 dfn-cert: DFN-CERT-2016-0451  
 dfn-cert: DFN-CERT-2016-0415  
 dfn-cert: DFN-CERT-2016-0403

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

```

Medium (CVSS: 5.3)

NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**

The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD): 80%****Vulnerability Detection Result**

The remote SSL/TLS server is using the following certificate(s) with a RSA key with less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):  
 1024:RSA:00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D  
 626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for C  
 omplication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no su  
 ... continues on next page ...

...continued from previous page ...
↔ch thing outside US,C=XX (Server certificate)
<b>Impact</b> Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace the certificate with a stronger key and reissue the certificates it signed.
<b>Vulnerability Insight</b> SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.
<b>Vulnerability Detection Method</b> Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit. Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048. ↳.. OID:1.3.6.1.4.1.25623.1.0.150710 Version used: 2021-12-10T12:48:00Z
<b>References</b> url: <a href="https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf">https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf</a>

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests
<b>Summary</b> The Mailserver on this host answers to VRFY and/or EXPN requests.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> 'VRFY root' produces the following answer: 252 2.0.0 root
<b>Solution:</b> <b>Solution type:</b> Workaround Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
... continues on next page ...



...continued from previous page ...
<b>Vulnerability Insight</b> VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.
<b>Vulnerability Detection Method</b> Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: 2023-10-31T05:06:37Z
<b>References</b> url: <a href="http://cr.yp.to/smtp/vrfy.html">http://cr.yp.to/smtp/vrfy.html</a>

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired
<b>Product detection result</b> cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)
<b>Summary</b> The remote server's SSL/TLS certificate has already expired.
<b>Quality of Detection (QoD): 99%</b>
<b>Vulnerability Detection Result</b> The certificate of the remote service expired on 2010-04-16 14:07:45. Certificate details: fingerprint (SHA-1)   ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256)   E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A ↪ F1E32DEE436DE813CC issued by   1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪ 30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX public key algorithm   RSA public key size (bits)   1024 serial   00FAF93A4C7FB6B9CC signature algorithm   sha1WithRSAEncryption subject   1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪ 30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX subject alternative names (SAN)   None
...continues on next page ...

...continued from previous page ...	
valid from	2010-03-17 14:07:45 UTC
valid until	2010-04-16 14:07:45 UTC
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace the SSL/TLS certificate by a new one.	
<b>Vulnerability Insight</b> This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.	
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2024-06-14T05:05:48Z	
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Collect and Report Certificate Details OID: 1.3.6.1.4.1.25623.1.0.103692)	

Medium (CVSS: 5.0)	
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	
<b>Summary</b> The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.	
<b>Quality of Detection (QoD):</b> 70%	
<b>Vulnerability Detection Result</b> The following indicates that the remote SSL/TLS service is affected: Protocol Version   Successful re-done SSL/TLS handshakes (Renegotiation) over an ↔ existing / already established SSL/TLS connection ----- ↔----- TLSv1.0   10	
<b>Impact</b> The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Users should contact their vendors for specific patch information.	
... continues on next page ...	

...continued from previous page ...
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
<b>Vulnerability Insight</b> The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: > It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.
<b>Vulnerability Detection Method</b> Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 Version used: 2024-09-27T05:05:23Z
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K14/0772 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112
Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<b>Product detection result</b>
... continues on next page ...

...continued from previous page ...
cpe:/a:ietf:transport_layer_security:1.0 Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> The service is only providing the deprecated TLSv1.0 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
<b>Impact</b> An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
<b>Solution:</b> <b>Solution type:</b> Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
<b>Vulnerability Detection Method</b> Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2024-09-27T05:05:23Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security:1.0 Method: SSL/TLS: Version Detection
... continues on next page ...

...continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2011-3389

cve: CVE-2015-0204

url: <https://ssl-config.mozilla.org/>url: <https://bettercrypto.org/>url: <https://datatracker.ietf.org/doc/rfc8996/>url: <https://vnhacker.blogspot.com/2011/09/beast.html>url: <https://web.archive.org/web/20201108095603/https://censys.io/blog/freak>url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters>  
↔-report-2014

cert-bund: WID-SEC-2023-1435

cert-bund: CB-K18/0799

cert-bund: CB-K16/1289

cert-bund: CB-K16/1096

cert-bund: CB-K15/1751

cert-bund: CB-K15/1266

cert-bund: CB-K15/0850

cert-bund: CB-K15/0764

cert-bund: CB-K15/0720

cert-bund: CB-K15/0548

cert-bund: CB-K15/0526

cert-bund: CB-K15/0509

cert-bund: CB-K15/0493

cert-bund: CB-K15/0384

cert-bund: CB-K15/0365

cert-bund: CB-K15/0364

cert-bund: CB-K15/0302

cert-bund: CB-K15/0192

cert-bund: CB-K15/0079

cert-bund: CB-K15/0016

cert-bund: CB-K14/1342

cert-bund: CB-K14/0231

dfn-cert: DFN-CERT-2020-0177

dfn-cert: DFN-CERT-2020-0111

dfn-cert: DFN-CERT-2019-0068

dfn-cert: DFN-CERT-2018-1441

dfn-cert: DFN-CERT-2018-1408

dfn-cert: DFN-CERT-2016-1372

dfn-cert: DFN-CERT-2016-1164

dfn-cert: DFN-CERT-2016-0388

dfn-cert: DFN-CERT-2015-1853

dfn-cert: DFN-CERT-2015-1332

dfn-cert: DFN-CERT-2015-0884

dfn-cert: DFN-CERT-2015-0800

... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2015-0758  
dfn-cert: DFN-CERT-2015-0567  
dfn-cert: DFN-CERT-2015-0544  
dfn-cert: DFN-CERT-2015-0530  
dfn-cert: DFN-CERT-2015-0396  
dfn-cert: DFN-CERT-2015-0375  
dfn-cert: DFN-CERT-2015-0374  
dfn-cert: DFN-CERT-2015-0305  
dfn-cert: DFN-CERT-2015-0199  
dfn-cert: DFN-CERT-2015-0079  
dfn-cert: DFN-CERT-2015-0021  
dfn-cert: DFN-CERT-2014-1414  
dfn-cert: DFN-CERT-2013-1847  
dfn-cert: DFN-CERT-2013-1792  
dfn-cert: DFN-CERT-2012-1979  
dfn-cert: DFN-CERT-2012-1829  
dfn-cert: DFN-CERT-2012-1530  
dfn-cert: DFN-CERT-2012-1380  
dfn-cert: DFN-CERT-2012-1377  
dfn-cert: DFN-CERT-2012-1292  
dfn-cert: DFN-CERT-2012-1214  
dfn-cert: DFN-CERT-2012-1213  
dfn-cert: DFN-CERT-2012-1180  
dfn-cert: DFN-CERT-2012-1156  
dfn-cert: DFN-CERT-2012-1155  
dfn-cert: DFN-CERT-2012-1039  
dfn-cert: DFN-CERT-2012-0956  
dfn-cert: DFN-CERT-2012-0908  
dfn-cert: DFN-CERT-2012-0868  
dfn-cert: DFN-CERT-2012-0867  
dfn-cert: DFN-CERT-2012-0848  
dfn-cert: DFN-CERT-2012-0838  
dfn-cert: DFN-CERT-2012-0776  
dfn-cert: DFN-CERT-2012-0722  
dfn-cert: DFN-CERT-2012-0638  
dfn-cert: DFN-CERT-2012-0627  
dfn-cert: DFN-CERT-2012-0451  
dfn-cert: DFN-CERT-2012-0418  
dfn-cert: DFN-CERT-2012-0354  
dfn-cert: DFN-CERT-2012-0234  
dfn-cert: DFN-CERT-2012-0221  
dfn-cert: DFN-CERT-2012-0177  
dfn-cert: DFN-CERT-2012-0170  
dfn-cert: DFN-CERT-2012-0146  
dfn-cert: DFN-CERT-2012-0142  
dfn-cert: DFN-CERT-2012-0126  
dfn-cert: DFN-CERT-2012-0123

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.3)

NVT: SSL/TLS: RSA Temporary Key Handling 'RSA\_EXPORT' Downgrade Issue (FREAK)

**Product detection result**

cpe:/a:ietf:transport\_layer\_security

Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↪802067)

**Summary**

This host is accepting 'RSA\_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD): 80%****Vulnerability Detection Result**

'RSA\_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:

TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

TLS\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5

TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5

'RSA\_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

TLS\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5

TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5

**Impact**

... continues on next page ...

...continued from previous page ...
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.
<b>Solution:</b> <b>Solution type:</b> VendorFix - Remove support for 'RSA_EXPORT' cipher suites from the service. - If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.
<b>Affected Software/OS</b> - Hosts accepting 'RSA_EXPORT' cipher suites - OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.
<b>Vulnerability Insight</b> Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.
<b>Vulnerability Detection Method</b> Check previous collected cipher suites saved in the KB. Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) OID:1.3.6.1.4.1.25623.1.0.805142 Version used: 2024-09-30T08:38:05Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)
<b>References</b> cve: CVE-2015-0204 url: <a href="https://freakattack.com">https://freakattack.com</a> url: <a href="http://www.securityfocus.com/bid/71936">http://www.securityfocus.com/bid/71936</a> url: <a href="http://secpod.org/blog/?p=3818">http://secpod.org/blog/?p=3818</a> url: <a href="http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac-toring-nsa.html">http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac-toring-nsa.html</a> cert-bund: CB-K18/0799 cert-bund: CB-K16/1289 cert-bund: CB-K16/1096 cert-bund: CB-K15/1751 cert-bund: CB-K15/1266 cert-bund: CB-K15/0850 cert-bund: CB-K15/0764 cert-bund: CB-K15/0720 cert-bund: CB-K15/0548
... continues on next page ...



...continued from previous page ...

```

cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021

```

Medium (CVSS: 4.0)

NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**

The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD): 80%****Vulnerability Detection Result**

The following certificates are part of the certificate chain but using insecure  
 ↪signature algorithms:

Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173  
 ↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic  
 ↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi  
 ↪ng outside US,C=XX

...continues on next page ...

...continued from previous page...	
<b>Signature Algorithm:</b>	sha1WithRSAEncryption
<b>Solution:</b> <b>Solution type:</b> Mitigation Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.	
<b>Vulnerability Insight</b> The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1 or fingerprint1, Fingerprint2	
<b>Vulnerability Detection Method</b> Check which hashing algorithm was used to sign the remote SSL/TLS certificate. Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm OID:1.3.6.1.4.1.25623.1.0.105880 Version used: 2021-10-15T11:13:32Z	
<b>References</b> url: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</a>	

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
<b>Summary</b> The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b>
... continues on next page ...

...continued from previous page ...
<b>Server Temporary Key Size: 1024 bits</b>
<b>Impact</b> An attacker might be able to decrypt the SSL/TLS communication offline.
<b>Solution:</b> <b>Solution type:</b> Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
<b>Vulnerability Insight</b> The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.
<b>Vulnerability Detection Method</b> Checks the DHE temporary public key size. Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↔... OID:1.3.6.1.4.1.25623.1.0.106223 Version used: 2024-09-30T08:38:05Z
<b>References</b> url: <a href="https://weakdh.org/">https://weakdh.org/</a> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a>

[ [return to 10.0.2.5](#) ]

### 2.1.18 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)
<b>Summary</b> TWiki is prone to a cross-site request forgery (CSRF) vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 01.Feb.2003
... continues on next page ...

...continued from previous page ...	
Fixed version:	4.3.2
<b>Impact</b> Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to TWiki version 4.3.2 or later.	
<b>Affected Software/OS</b> TWiki version prior to 4.3.2	
<b>Vulnerability Insight</b> Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.	
<b>Vulnerability Detection Method</b> Details: TWiki Cross-Site Request Forgery Vulnerability (Sep 2010) OID:1.3.6.1.4.1.25623.1.0.801281 Version used: 2024-03-01T14:37:10Z	
<b>References</b> cve: CVE-2009-4898 url: <a href="http://www.openwall.com/lists/oss-security/2010/08/03/8">http://www.openwall.com/lists/oss-security/2010/08/03/8</a> url: <a href="http://www.openwall.com/lists/oss-security/2010/08/02/17">http://www.openwall.com/lists/oss-security/2010/08/02/17</a> url: <a href="http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix">http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix</a> url: <a href="http://twiki.org/cgi-bin/view/Codev/DownloadTWiki">http://twiki.org/cgi-bin/view/Codev/DownloadTWiki</a>	

Medium (CVSS: 6.1)	
NVT: jQuery < 1.9.0 XSS Vulnerability	
<b>Summary</b> jQuery is prone to a cross-site scripting (XSS) vulnerability.	
<b>Quality of Detection (QoD):</b> 80%	
<b>Vulnerability Detection Result</b> Installed version: 1.3.2 Fixed version: 1.9.0 Installation path / port: /mutillidae/javascript/ddsmoothmenu/jquery.min.js Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):	
...continues on next page ...	

...continued from previous page ...
<ul style="list-style-type: none"> <li>- Identified file: <code>http://10.0.2.5/mutillidae/javascript/ddsmoothmenu/jquery.min↵.js</code></li> <li>- Referenced at: <code>http://10.0.2.5/mutillidae/</code></li> </ul>
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 1.9.0 or later.
<b>Affected Software/OS</b> jQuery prior to version 1.9.0.
<b>Vulnerability Insight</b> The <code>jQuery(strInput)</code> function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the ' <code>&lt;</code> ' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the ' <code>&lt;</code> ' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: jQuery < 1.9.0 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.141636 Version used: 2023-07-14T05:06:08Z
<b>References</b> cve: CVE-2012-6708 url: <a href="https://bugs.jquery.com/ticket/11290">https://bugs.jquery.com/ticket/11290</a> cert-bund: WID-SEC-2022-0673 cert-bund: CB-K22/0045 cert-bund: CB-K18/1131 dfn-cert: DFN-CERT-2023-1197 dfn-cert: DFN-CERT-2020-0590

Medium (CVSS: 6.1)
NVT: TWiki < 6.1.0 XSS Vulnerability
<b>Summary</b> bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Installed version: 01.Feb.2003
... continues on next page ...

...continued from previous page ...	
<b>Fixed version:</b>	6.1.0
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 6.1.0 or later.	
<b>Affected Software/OS</b> TWiki version 6.0.2 and probably prior.	
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: TWiki < 6.1.0 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.141830 Version used: 2023-07-14T16:09:27Z	
<b>References</b> cve: CVE-2018-20212 url: <a href="https://seclists.org/fulldisclosure/2019/Jan/7">https://seclists.org/fulldisclosure/2019/Jan/7</a> url: <a href="http://twiki.org/cgi-bin/view/Codev/DownloadTWiki">http://twiki.org/cgi-bin/view/Codev/DownloadTWiki</a>	

Medium (CVSS: 6.0)	
NVT: TWiki CSRF Vulnerability	
<b>Summary</b> TWiki is prone to a cross-site request forgery (CSRF) vulnerability.	
<b>Quality of Detection (QoD):</b> 80%	
<b>Vulnerability Detection Result</b> Installed version: 01.Feb.2003 Fixed version: 4.3.1	
<b>Impact</b> Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to version 4.3.1 or later.	
<b>Affected Software/OS</b> TWiki version prior to 4.3.1	
... continues on next page ...	

...continued from previous page ...
<b>Vulnerability Insight</b> Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.
<b>Vulnerability Detection Method</b> Details: TWiki CSRF Vulnerability OID:1.3.6.1.4.1.25623.1.0.800400 Version used: 2024-06-28T05:05:33Z
<b>References</b> cve: CVE-2009-1339 url: <a href="http://secunia.com/advisories/34880">http://secunia.com/advisories/34880</a> url: <a href="http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258">http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258</a> url: <a href="http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff-cv2-cve-2009-1339.txt">http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff-cv2-cve-2009-1339.txt</a>

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled
<b>Summary</b> The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> The web server has the following HTTP methods enabled: TRACE
<b>Impact</b> An attacker may use this flaw to trick your legitimate web users to give him their credentials.
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information.
<b>Affected Software/OS</b> Web servers with enabled TRACE and/or TRACK methods.
<b>Vulnerability Insight</b> ... continues on next page ...

...continued from previous page ...

It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

#### Vulnerability Detection Method

Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.

Details: HTTP Debugging Methods (TRACE/TRACK) Enabled

OID:1.3.6.1.4.1.25623.1.0.11213

Version used: 2023-08-01T13:29:10Z

#### References

cve: CVE-2003-1567

cve: CVE-2004-2320

cve: CVE-2004-2763

cve: CVE-2005-3398

cve: CVE-2006-4683

cve: CVE-2007-3008

cve: CVE-2008-7253

cve: CVE-2009-2823

cve: CVE-2010-0386

cve: CVE-2012-2223

cve: CVE-2014-7883

url: <http://www.kb.cert.org/vuls/id/288308>

url: <http://www.securityfocus.com/bid/11604>

url: <http://www.securityfocus.com/bid/15222>

url: <http://www.securityfocus.com/bid/19915>

url: <http://www.securityfocus.com/bid/24456>

url: <http://www.securityfocus.com/bid/33374>

url: <http://www.securityfocus.com/bid/36956>

url: <http://www.securityfocus.com/bid/36990>

url: <http://www.securityfocus.com/bid/37995>

url: <http://www.securityfocus.com/bid/9506>

url: <http://www.securityfocus.com/bid/9561>

url: <http://www.kb.cert.org/vuls/id/867593>

url: <https://httpd.apache.org/docs/current/en/mod/core.html#traceenable>

url: <https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trace-verbs/ba-p/784482>

url: [https://owasp.org/www-community/attacks/Cross\\_Site\\_Tracing](https://owasp.org/www-community/attacks/Cross_Site_Tracing)

cert-bund: CB-K14/0981

dfn-cert: DFN-CERT-2021-1825

dfn-cert: DFN-CERT-2014-1018

dfn-cert: DFN-CERT-2010-0020



Medium (CVSS: 5.3)
NVT: phpinfo() Output Reporting (HTTP)
<p><b>Summary</b></p> <p>Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.</p>
<p><b>Quality of Detection (QoD): 80%</b></p>
<p><b>Vulnerability Detection Result</b></p> <p>The following files are calling the function phpinfo() which disclose potentially sensitive information:</p> <p>http://10.0.2.5/mutillidae/phpinfo.php</p> <p>Concluded from:</p> <pre>&lt;title&gt;phpinfo()&lt;/title&gt;&lt;meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV E" /&gt;&lt;/head&gt; &lt;tr&gt;&lt;td class="e"&gt;Configuration File (php.ini) Path &lt;/td&gt;&lt;td class="v"&gt;/etc/ph p5/cgi &lt;/td&gt;&lt;/tr&gt; &lt;h2&gt;PHP Variables&lt;/h2&gt;</pre> <p>http://10.0.2.5/phpinfo.php</p> <p>Concluded from:</p> <pre>&lt;title&gt;phpinfo()&lt;/title&gt;&lt;meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV E" /&gt;&lt;/head&gt; &lt;tr&gt;&lt;td class="e"&gt;Configuration File (php.ini) Path &lt;/td&gt;&lt;td class="v"&gt;/etc/ph p5/cgi &lt;/td&gt;&lt;/tr&gt; &lt;h2&gt;PHP Variables&lt;/h2&gt;</pre>
<p><b>Impact</b></p> <p>Some of the information that can be gathered from this file includes:</p> <p>The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Workaround</p> <p>Delete the listed files or restrict access to them.</p>
<p><b>Affected Software/OS</b></p> <p>All systems exposing a file containing the output of the phpinfo() PHP function.</p> <p>This VT is also reporting if an affected endpoint for the following products have been identified:</p> <ul style="list-style-type: none"> <li>- CVE-2008-0149: TUTOS</li> <li>- CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK</li> </ul>
<p><b>Vulnerability Insight</b></p> <p>... continues on next page ...</p>

...continued from previous page ...
Many PHP installation tutorials instruct the user to create a file called <code>phpinfo.php</code> or similar containing the <code>phpinfo()</code> statement. Such a file is often left back in the webserver directory.
<b>Vulnerability Detection Method</b> This script reports files identified by the following separate VT: 'phpinfo() Output Detection (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.108474). Details: <code>phpinfo()</code> Output Reporting (HTTP) OID: 1.3.6.1.4.1.25623.1.0.11229 Version used: 2024-12-17T05:05:41Z
<b>References</b> cve: CVE-2008-0149 cve: CVE-2023-49282 cve: CVE-2023-49283 url: <a href="https://www.php.net/manual/en/function.phpinfo.php">https://www.php.net/manual/en/function.phpinfo.php</a>

Medium (CVSS: 5.0)
NVT: <code>/doc directory browsable</code>
<b>Summary</b> The <code>/doc</code> directory is browsable. <code>/doc</code> shows the content of the <code>/usr/doc</code> directory and therefore it shows which programs and - important! - the version of the installed programs.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerable URL: <code>http://10.0.2.5/doc/</code>
<b>Solution:</b> <b>Solution type:</b> Mitigation Use access restrictions for the <code>/doc</code> directory. If you use Apache you might use this in your <code>access.conf</code> : <pre>&lt;Directory /usr/doc&gt; AllowOverride None order deny, allow deny from all allow from localhost &lt;/Directory&gt;</pre>
<b>Vulnerability Detection Method</b> Details: <code>/doc directory browsable</code> OID: 1.3.6.1.4.1.25623.1.0.10056 Version used: 2023-08-01T13:29:10Z
<b>References</b> cve: CVE-1999-0678 url: <a href="http://www.securityfocus.com/bid/318">http://www.securityfocus.com/bid/318</a>

Medium (CVSS: 5.0)
NVT: awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check
<b>Summary</b> awiki is prone to multiple local file include (LFI) vulnerabilities because it fails to properly sanitize user-supplied input.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> Vulnerable URL: <a href="http://10.0.2.5/mutillidae/index.php?page=/etc/passwd">http://10.0.2.5/mutillidae/index.php?page=/etc/passwd</a>
<b>Impact</b> An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host.
<b>Solution:</b> <b>Solution type:</b> WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
<b>Affected Software/OS</b> awiki version 20100125 and prior.
<b>Vulnerability Detection Method</b> Sends a crafted HTTP GET request and checks the response. Details: awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check OID:1.3.6.1.4.1.25623.1.0.103210 Version used: 2023-12-13T05:05:23Z
<b>References</b> url: <a href="https://www.exploit-db.com/exploits/36047/">https://www.exploit-db.com/exploits/36047/</a> url: <a href="http://www.securityfocus.com/bid/49187">http://www.securityfocus.com/bid/49187</a>

Medium (CVSS: 5.0)
NVT: QWikiwiki directory traversal vulnerability
<b>Summary</b> The remote host is running QWikiwiki, a Wiki application written in PHP. The remote version of this software contains a validation input flaw which may allow an attacker to use it to read arbitrary files on the remote host with the privileges of the web server.
... continues on next page ...

...continued from previous page ...
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> Vulnerable URL: http://10.0.2.5/mutillidae/index.php?page=../../../../../../../../.. ↪../../../../etc/passwd%00
<b>Solution:</b> <b>Solution type:</b> WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
<b>Vulnerability Detection Method</b> Details: QWikiwiki directory traversal vulnerability OID:1.3.6.1.4.1.25623.1.0.16100 Version used: 2023-12-13T05:05:23Z
<b>References</b> cve: CVE-2005-0283 url: http://www.securityfocus.com/bid/12163

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP
<b>Summary</b> The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following input fields were identified (URL:input name): http://10.0.2.5/dvwa/login.php:password http://10.0.2.5/phpMyAdmin/:pma_password http://10.0.2.5/phpMyAdmin/?D=A:pma_password http://10.0.2.5/tikiwiki/tiki-install.php:pass http://10.0.2.5/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword
<b>Impact</b> An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
... continues on next page ...

...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> Workaround Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
<b>Affected Software/OS</b> Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
<b>Vulnerability Detection Method</b> Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password' Details: Cleartext Transmission of Sensitive Information via HTTP OID:1.3.6.1.4.1.25623.1.0.108440 Version used: 2023-09-07T05:05:21Z
<b>References</b> url: <a href="https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management">https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</a> url: <a href="https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure">https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</a> url: <a href="https://cwe.mitre.org/data/definitions/319.html">https://cwe.mitre.org/data/definitions/319.html</a>

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
<b>Summary</b> phpMyAdmin is prone to a cross-site scripting (XSS) vulnerability.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.
<b>Solution:</b> <b>Solution type:</b> WillNotFix
... continues on next page ...

...continued from previous page ...
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
<b>Affected Software/OS</b> phpMyAdmin version 3.3.8.1 and prior.
<b>Vulnerability Insight</b> The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.
<b>Vulnerability Detection Method</b> Details: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability OID:1.3.6.1.4.1.25623.1.0.801660 Version used: 2023-10-17T05:05:34Z
<b>References</b> cve: CVE-2010-4480 url: <a href="http://www.exploit-db.com/exploits/15699/">http://www.exploit-db.com/exploits/15699/</a> url: <a href="http://www.vupen.com/english/advisories/2010/3133">http://www.vupen.com/english/advisories/2010/3133</a> dfn-cert: DFN-CERT-2011-0467 dfn-cert: DFN-CERT-2011-0451 dfn-cert: DFN-CERT-2011-0016 dfn-cert: DFN-CERT-2011-0002

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability
<b>Summary</b> jQuery is prone to a cross-site scripting (XSS) vulnerability.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> Installed version: 1.3.2 Fixed version: 1.6.3 Installation path / port: /mutillidae/javascript/ddsmoothmenu/jquery.min.js Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info): - Identified file: <a href="http://10.0.2.5/mutillidae/javascript/ddsmoothmenu/jquery.min.js">http://10.0.2.5/mutillidae/javascript/ddsmoothmenu/jquery.min.js</a> ↪.js - Referenced at: <a href="http://10.0.2.5/mutillidae/">http://10.0.2.5/mutillidae/</a>
... continues on next page ...

...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 1.6.3 or later.
<b>Affected Software/OS</b> jQuery prior to version 1.6.3.
<b>Vulnerability Insight</b> Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: jQuery < 1.6.3 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.141637 Version used: 2023-07-14T05:06:08Z
<b>References</b> cve: CVE-2011-4969 url: <a href="https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/">https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/</a> cert-bund: CB-K17/0195 dfn-cert: DFN-CERT-2017-0199 dfn-cert: DFN-CERT-2016-0890

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
<b>Product detection result</b> cpe:/a:apache:http_server:2.2.8 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↪.0.117232)
<b>Summary</b> Apache HTTP Server is prone to a cookie information disclosure vulnerability.
<b>Quality of Detection (QoD):</b> 99%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> ... continues on next page ...

...continued from previous page ...
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to Apache HTTP Server version 2.2.22 or later.
<b>Affected Software/OS</b> Apache HTTP Server versions 2.2.0 through 2.2.21.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.902830 Version used: 2022-04-27T12:01:52Z
<b>Product Detection Result</b> Product: cpe:/a:apache:http_server:2.2.8 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
<b>References</b> cve: CVE-2012-0053 url: <a href="http://secunia.com/advisories/47779">http://secunia.com/advisories/47779</a> url: <a href="http://www.securityfocus.com/bid/51706">http://www.securityfocus.com/bid/51706</a> url: <a href="http://www.exploit-db.com/exploits/18442">http://www.exploit-db.com/exploits/18442</a> url: <a href="http://rhn.redhat.com/errata/RHSA-2012-0128.html">http://rhn.redhat.com/errata/RHSA-2012-0128.html</a> url: <a href="http://httpd.apache.org/security/vulnerabilities_22.html">http://httpd.apache.org/security/vulnerabilities_22.html</a> url: <a href="http://svn.apache.org/viewvc?view=revision&amp;revision=1235454">http://svn.apache.org/viewvc?view=revision&amp;revision=1235454</a> url: <a href="http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html">http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html</a> cert-bund: CB-K15/0080 cert-bund: CB-K14/1505 cert-bund: CB-K14/0608 dfn-cert: DFN-CERT-2015-0082 dfn-cert: DFN-CERT-2014-1592 dfn-cert: DFN-CERT-2014-0635 dfn-cert: DFN-CERT-2013-1307 dfn-cert: DFN-CERT-2012-1276 dfn-cert: DFN-CERT-2012-1112 dfn-cert: DFN-CERT-2012-0928 dfn-cert: DFN-CERT-2012-0758 dfn-cert: DFN-CERT-2012-0744
... continues on next page ...



...continued from previous page ...
dfn-cert: DFN-CERT-2012-0568
dfn-cert: DFN-CERT-2012-0425
dfn-cert: DFN-CERT-2012-0424
dfn-cert: DFN-CERT-2012-0387
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
dfn-cert: DFN-CERT-2012-0306
dfn-cert: DFN-CERT-2012-0264
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188

[\[ return to 10.0.2.5 \]](#)

### 2.1.19 Medium 5432/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
<b>Product detection result</b> cpe:/a:ietf:transport_layer_security:1.0 Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
<b>Summary</b> It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto ↪col and supports one or more ciphers. Those supported ciphers can be found in ↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020 ↪67) VT.
<b>Impact</b> An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
<b>Solution:</b> <b>Solution type:</b> Mitigation
... continues on next page ...

...continued from previous page ...
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
<b>Affected Software/OS</b> All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
<b>Vulnerability Insight</b> The SSLv2 and SSLv3 protocols contain known cryptographic flaws like: - CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE) - CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)
<b>Vulnerability Detection Method</b> Check the used SSL protocols of the services provided by this system. Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection OID: 1.3.6.1.4.1.25623.1.0.111012 Version used: 2024-09-27T05:05:23Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security:1.0 Method: SSL/TLS: Version Detection OID: 1.3.6.1.4.1.25623.1.0.105782)
<b>References</b> cve: CVE-2016-0800 cve: CVE-2014-3566 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://drownattack.com/">https://drownattack.com/</a> url: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-report-2014 cert-bund: WID-SEC-2023-0431 cert-bund: WID-SEC-2023-0427 cert-bund: CB-K18/0094 cert-bund: CB-K17/1198 cert-bund: CB-K17/1196 cert-bund: CB-K16/1828 cert-bund: CB-K16/1438 cert-bund: CB-K16/1384 cert-bund: CB-K16/1141 cert-bund: CB-K16/1107 cert-bund: CB-K16/1102 cert-bund: CB-K16/0792 cert-bund: CB-K16/0599 cert-bund: CB-K16/0597
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K16/0459  
cert-bund: CB-K16/0456  
cert-bund: CB-K16/0433  
cert-bund: CB-K16/0424  
cert-bund: CB-K16/0415  
cert-bund: CB-K16/0413  
cert-bund: CB-K16/0374  
cert-bund: CB-K16/0367  
cert-bund: CB-K16/0331  
cert-bund: CB-K16/0329  
cert-bund: CB-K16/0328  
cert-bund: CB-K16/0156  
cert-bund: CB-K15/1514  
cert-bund: CB-K15/1358  
cert-bund: CB-K15/1021  
cert-bund: CB-K15/0972  
cert-bund: CB-K15/0637  
cert-bund: CB-K15/0590  
cert-bund: CB-K15/0525  
cert-bund: CB-K15/0393  
cert-bund: CB-K15/0384  
cert-bund: CB-K15/0287  
cert-bund: CB-K15/0252  
cert-bund: CB-K15/0246  
cert-bund: CB-K15/0237  
cert-bund: CB-K15/0118  
cert-bund: CB-K15/0110  
cert-bund: CB-K15/0108  
cert-bund: CB-K15/0080  
cert-bund: CB-K15/0078  
cert-bund: CB-K15/0077  
cert-bund: CB-K15/0075  
cert-bund: CB-K14/1617  
cert-bund: CB-K14/1581  
cert-bund: CB-K14/1537  
cert-bund: CB-K14/1479  
cert-bund: CB-K14/1458  
cert-bund: CB-K14/1342  
cert-bund: CB-K14/1314  
cert-bund: CB-K14/1313  
cert-bund: CB-K14/1311  
cert-bund: CB-K14/1304  
cert-bund: CB-K14/1296  
dfn-cert: DFN-CERT-2018-0096  
dfn-cert: DFN-CERT-2017-1238  
dfn-cert: DFN-CERT-2017-1236  
dfn-cert: DFN-CERT-2016-1929

...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2016-1527  
dfn-cert: DFN-CERT-2016-1468  
dfn-cert: DFN-CERT-2016-1216  
dfn-cert: DFN-CERT-2016-1174  
dfn-cert: DFN-CERT-2016-1168  
dfn-cert: DFN-CERT-2016-0884  
dfn-cert: DFN-CERT-2016-0841  
dfn-cert: DFN-CERT-2016-0644  
dfn-cert: DFN-CERT-2016-0642  
dfn-cert: DFN-CERT-2016-0496  
dfn-cert: DFN-CERT-2016-0495  
dfn-cert: DFN-CERT-2016-0465  
dfn-cert: DFN-CERT-2016-0459  
dfn-cert: DFN-CERT-2016-0453  
dfn-cert: DFN-CERT-2016-0451  
dfn-cert: DFN-CERT-2016-0415  
dfn-cert: DFN-CERT-2016-0403  
dfn-cert: DFN-CERT-2016-0388  
dfn-cert: DFN-CERT-2016-0360  
dfn-cert: DFN-CERT-2016-0359  
dfn-cert: DFN-CERT-2016-0357  
dfn-cert: DFN-CERT-2016-0171  
dfn-cert: DFN-CERT-2015-1431  
dfn-cert: DFN-CERT-2015-1075  
dfn-cert: DFN-CERT-2015-1026  
dfn-cert: DFN-CERT-2015-0664  
dfn-cert: DFN-CERT-2015-0548  
dfn-cert: DFN-CERT-2015-0404  
dfn-cert: DFN-CERT-2015-0396  
dfn-cert: DFN-CERT-2015-0259  
dfn-cert: DFN-CERT-2015-0254  
dfn-cert: DFN-CERT-2015-0245  
dfn-cert: DFN-CERT-2015-0118  
dfn-cert: DFN-CERT-2015-0114  
dfn-cert: DFN-CERT-2015-0083  
dfn-cert: DFN-CERT-2015-0082  
dfn-cert: DFN-CERT-2015-0081  
dfn-cert: DFN-CERT-2015-0076  
dfn-cert: DFN-CERT-2014-1717  
dfn-cert: DFN-CERT-2014-1680  
dfn-cert: DFN-CERT-2014-1632  
dfn-cert: DFN-CERT-2014-1564  
dfn-cert: DFN-CERT-2014-1542  
dfn-cert: DFN-CERT-2014-1414  
dfn-cert: DFN-CERT-2014-1366  
dfn-cert: DFN-CERT-2014-1354

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites
<b>Product detection result</b> cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↪802067)
<b>Summary</b> This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
<b>Quality of Detection (QoD):</b> 98%
<b>Vulnerability Detection Result</b> 'Weak' cipher suites accepted by this service via the SSLv3 protocol: TLS_RSA_WITH_RC4_128_SHA 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_SHA
<b>Solution:</b> <b>Solution type:</b> Mitigation The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.
<b>Vulnerability Insight</b> These rules are applied for the evaluation of the cryptographic strength: <ul style="list-style-type: none"> <li>- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)</li> <li>- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)</li> <li>- 1024 bit RSA authentication is considered to be insecure and therefore as weak</li> <li>- Any cipher considered to be secure for only the next 10 years is considered as medium</li> <li>- Any other cipher is considered as strong</li> </ul>
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: 2024-09-27T05:05:23Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security ... continues on next page ...

...continued from previous page ...
Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)
<b>References</b> cve: CVE-2013-2566 cve: CVE-2015-2808 cve: CVE-2015-4000 url: <a href="https://www.bsi.bund.de/SharedDocs/Warntmeldungen/DE/CB/warntmeldung_cb-k16-1-465_update_6.html">https://www.bsi.bund.de/SharedDocs/Warntmeldungen/DE/CB/warntmeldung_cb-k16-1-465_update_6.html</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a> cert-bund: CB-K21/0067 cert-bund: CB-K19/0812 cert-bund: CB-K17/1750 cert-bund: CB-K16/1593 cert-bund: CB-K16/1552 cert-bund: CB-K16/1102 cert-bund: CB-K16/0617 cert-bund: CB-K16/0599 cert-bund: CB-K16/0168 cert-bund: CB-K16/0121 cert-bund: CB-K16/0090 cert-bund: CB-K16/0030 cert-bund: CB-K15/1751 cert-bund: CB-K15/1591 cert-bund: CB-K15/1550 cert-bund: CB-K15/1517 cert-bund: CB-K15/1514 cert-bund: CB-K15/1464 cert-bund: CB-K15/1442 cert-bund: CB-K15/1334 cert-bund: CB-K15/1269 cert-bund: CB-K15/1136 cert-bund: CB-K15/1090 cert-bund: CB-K15/1059 cert-bund: CB-K15/1022 cert-bund: CB-K15/1015 cert-bund: CB-K15/0986 cert-bund: CB-K15/0964 cert-bund: CB-K15/0962 cert-bund: CB-K15/0932 cert-bund: CB-K15/0927 cert-bund: CB-K15/0926 cert-bund: CB-K15/0907 cert-bund: CB-K15/0901 cert-bund: CB-K15/0896
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0889  
 cert-bund: CB-K15/0877  
 cert-bund: CB-K15/0850  
 cert-bund: CB-K15/0849  
 cert-bund: CB-K15/0834  
 cert-bund: CB-K15/0827  
 cert-bund: CB-K15/0802  
 cert-bund: CB-K15/0764  
 cert-bund: CB-K15/0733  
 cert-bund: CB-K15/0667  
 cert-bund: CB-K14/0935  
 dfn-cert: DFN-CERT-2023-2939  
 dfn-cert: DFN-CERT-2021-0775  
 dfn-cert: DFN-CERT-2020-1561  
 dfn-cert: DFN-CERT-2020-1276  
 dfn-cert: DFN-CERT-2017-1821  
 dfn-cert: DFN-CERT-2016-1692  
 dfn-cert: DFN-CERT-2016-1648  
 dfn-cert: DFN-CERT-2016-1168  
 dfn-cert: DFN-CERT-2016-0665  
 dfn-cert: DFN-CERT-2016-0642  
 dfn-cert: DFN-CERT-2016-0184  
 dfn-cert: DFN-CERT-2016-0135  
 dfn-cert: DFN-CERT-2016-0101  
 dfn-cert: DFN-CERT-2016-0035  
 dfn-cert: DFN-CERT-2015-1853  
 dfn-cert: DFN-CERT-2015-1679  
 dfn-cert: DFN-CERT-2015-1632  
 dfn-cert: DFN-CERT-2015-1608  
 dfn-cert: DFN-CERT-2015-1542  
 dfn-cert: DFN-CERT-2015-1518  
 dfn-cert: DFN-CERT-2015-1406  
 dfn-cert: DFN-CERT-2015-1341  
 dfn-cert: DFN-CERT-2015-1194  
 dfn-cert: DFN-CERT-2015-1144  
 dfn-cert: DFN-CERT-2015-1113  
 dfn-cert: DFN-CERT-2015-1078  
 dfn-cert: DFN-CERT-2015-1067  
 dfn-cert: DFN-CERT-2015-1038  
 dfn-cert: DFN-CERT-2015-1016  
 dfn-cert: DFN-CERT-2015-1012  
 dfn-cert: DFN-CERT-2015-0980  
 dfn-cert: DFN-CERT-2015-0977  
 dfn-cert: DFN-CERT-2015-0976  
 dfn-cert: DFN-CERT-2015-0960  
 dfn-cert: DFN-CERT-2015-0956  
 dfn-cert: DFN-CERT-2015-0944

...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits
<b>Summary</b> The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The remote SSL/TLS server is using the following certificate(s) with a RSA key with less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer): 1024:RSA:00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX (Server certificate)
<b>Impact</b> Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace the certificate with a stronger key and reissue the certificates it signed.
<b>Vulnerability Insight</b> SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.
<b>Vulnerability Detection Method</b> Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit. Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
... continues on next page ...



...continued from previous page ...
↔...
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z
<b>References</b>
url: <a href="https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf">https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf</a>

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
<b>Summary</b> The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> The following indicates that the remote SSL/TLS service is affected: Protocol Version   Successful re-done SSL/TLS handshakes (Renegotiation) over an ↔ existing / already established SSL/TLS connection ----- ↔----- TLSv1.0   10
<b>Impact</b> The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.
<b>Solution:</b> <b>Solution type:</b> VendorFix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
<b>Vulnerability Insight</b> The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: > It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
... continues on next page ...

...continued from previous page ...
Both CVEs are still kept in this VT as a reference to the origin of this flaw.
<div><b>Vulnerability Detection Method</b> Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 Version used: 2024-09-27T05:05:23Z</div>
<div><b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K14/0772 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112</div>
Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired
<div><b>Product detection result</b> cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)</div>
<div><b>Summary</b> The remote server's SSL/TLS certificate has already expired.</div>
Quality of Detection (QoD): 99%
<div><b>Vulnerability Detection Result</b> The certificate of the remote service expired on 2010-04-16 14:07:45. Certificate details: fingerprint (SHA-1)   ED093088706603BFD5DC237399B498DA2D4D31C6</div>
... continues on next page ...

...continued from previous page...	
fingerprint (SHA-256) ↪F1E32DEE436DE813CC	E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A
issued by ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX	1.2.840.113549.1.9.1=#726F6F74407562756E747538
public key algorithm	RSA
public key size (bits)	1024
serial	00FAF93A4C7FB6B9CC
signature algorithm	sha1WithRSAEncryption
subject ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX	1.2.840.113549.1.9.1=#726F6F74407562756E747538
subject alternative names (SAN)	None
valid from	2010-03-17 14:07:45 UTC
valid until	2010-04-16 14:07:45 UTC
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace the SSL/TLS certificate by a new one.	
<b>Vulnerability Insight</b> This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.	
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2024-06-14T05:05:48Z	
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Collect and Report Certificate Details OID: 1.3.6.1.4.1.25623.1.0.103692)	
Medium (CVSS: 4.3)	
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	
<b>Product detection result</b> cpe:/a:ietf:transport_layer_security:1.0 Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)	
...continues on next page...	

...continued from previous page ...
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> The service is only providing the deprecated TLSv1.0 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
<b>Impact</b> An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
<b>Solution:</b> <b>Solution type:</b> Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
<b>Vulnerability Detection Method</b> Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2024-09-27T05:05:23Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security:1.0 Method: SSL/TLS: Version Detection OID: 1.3.6.1.4.1.25623.1.0.105782)
<b>References</b> cve: CVE-2011-3389
... continues on next page ...

...continued from previous page...

```

cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↔-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396

```

...continues on next page...

...continued from previous page ...

dfn-cert: DFN-CERT-2015-0375  
dfn-cert: DFN-CERT-2015-0374  
dfn-cert: DFN-CERT-2015-0305  
dfn-cert: DFN-CERT-2015-0199  
dfn-cert: DFN-CERT-2015-0079  
dfn-cert: DFN-CERT-2015-0021  
dfn-cert: DFN-CERT-2014-1414  
dfn-cert: DFN-CERT-2013-1847  
dfn-cert: DFN-CERT-2013-1792  
dfn-cert: DFN-CERT-2012-1979  
dfn-cert: DFN-CERT-2012-1829  
dfn-cert: DFN-CERT-2012-1530  
dfn-cert: DFN-CERT-2012-1380  
dfn-cert: DFN-CERT-2012-1377  
dfn-cert: DFN-CERT-2012-1292  
dfn-cert: DFN-CERT-2012-1214  
dfn-cert: DFN-CERT-2012-1213  
dfn-cert: DFN-CERT-2012-1180  
dfn-cert: DFN-CERT-2012-1156  
dfn-cert: DFN-CERT-2012-1155  
dfn-cert: DFN-CERT-2012-1039  
dfn-cert: DFN-CERT-2012-0956  
dfn-cert: DFN-CERT-2012-0908  
dfn-cert: DFN-CERT-2012-0868  
dfn-cert: DFN-CERT-2012-0867  
dfn-cert: DFN-CERT-2012-0848  
dfn-cert: DFN-CERT-2012-0838  
dfn-cert: DFN-CERT-2012-0776  
dfn-cert: DFN-CERT-2012-0722  
dfn-cert: DFN-CERT-2012-0638  
dfn-cert: DFN-CERT-2012-0627  
dfn-cert: DFN-CERT-2012-0451  
dfn-cert: DFN-CERT-2012-0418  
dfn-cert: DFN-CERT-2012-0354  
dfn-cert: DFN-CERT-2012-0234  
dfn-cert: DFN-CERT-2012-0221  
dfn-cert: DFN-CERT-2012-0177  
dfn-cert: DFN-CERT-2012-0170  
dfn-cert: DFN-CERT-2012-0146  
dfn-cert: DFN-CERT-2012-0142  
dfn-cert: DFN-CERT-2012-0126  
dfn-cert: DFN-CERT-2012-0123  
dfn-cert: DFN-CERT-2012-0095  
dfn-cert: DFN-CERT-2012-0051  
dfn-cert: DFN-CERT-2012-0047  
dfn-cert: DFN-CERT-2012-0021  
dfn-cert: DFN-CERT-2011-1953

...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
<b>Summary</b> The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Server Temporary Key Size: 1024 bits
<b>Impact</b> An attacker might be able to decrypt the SSL/TLS communication offline.
<b>Solution:</b> <b>Solution type:</b> Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
<b>Vulnerability Insight</b> The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.
<b>Vulnerability Detection Method</b> Checks the DHE temporary public key size. Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↪.. OID:1.3.6.1.4.1.25623.1.0.106223
... continues on next page ...

...continued from previous page ...
Version used: 2024-09-30T08:38:05Z
<b>References</b> url: <a href="https://weakdh.org/">https://weakdh.org/</a> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a>

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
<b>Summary</b> The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following certificates are part of the certificate chain but using insecure ↪signature algorithms: Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173 ↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic ↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi ↪ng outside US,C=XX Signature Algorithm: sha1WithRSAEncryption
<b>Solution:</b> <b>Solution type:</b> Mitigation Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.
<b>Vulnerability Insight</b> The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: <ul style="list-style-type: none"> <li>- Secure Hash Algorithm 1 (SHA-1)</li> <li>- Message Digest 5 (MD5)</li> <li>- Message Digest 4 (MD4)</li> <li>- Message Digest 2 (MD2)</li> </ul> Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1
... continues on next page ...



...continued from previous page ...
or fingerprint1, Fingerprint2
<b>Vulnerability Detection Method</b> Check which hashing algorithm was used to sign the remote SSL/TLS certificate. Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm OID:1.3.6.1.4.1.25623.1.0.105880 Version used: 2021-10-15T11:13:32Z
<b>References</b> url: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</a>

[\[ return to 10.0.2.5 \]](#)

### 2.1.20 Medium 23/tcp

Medium (CVSS: 4.8) NVT: Telnet Unencrypted Cleartext Login
<b>Summary</b> The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace Telnet with a protocol like SSH which supports encrypted connections.
<b>Vulnerability Detection Method</b> Details: Telnet Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108522 Version used: 2023-10-13T05:06:09Z

[\[ return to 10.0.2.5 \]](#)

2.1.21 Medium 445/tcp

Medium (CVSS: 6.0)
NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check
<div>Product detection result</div> <div>cpe:/a:samba:samba:3.0.20</div> <div>Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)</div>
<div>Summary</div> <div>Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.</div>
<div>Quality of Detection (QoD): 99%</div>
<div>Vulnerability Detection Result</div> <div>By sending a special crafted SMB request it was possible to execute ‘‘ping -p 5f ↪4f70656e564153565432353834375f -c50 10.0.2.15’’ on the remote host.</div> <div>Received answer (ICMP "Data" field):</div> <div><div><div>0x00:</div><div>FF 06 78 67 6C C0 05 00 56 54 32 35 38 34 37 5F</div><div>..xgl...VT25847_</div></div><div><div>0x10:</div><div>5F 4F 70 65 6E 56 41 53 56 54 32 35 38 34 37 5F</div><div>_OpenVASVT25847_</div></div><div><div>0x20:</div><div>5F 4F 70 65 6E 56 41 53 56 54 32 35 38 34 37 5F</div><div>_OpenVASVT25847_</div></div><div><div>0x30:</div><div>5F 4F 70 65 6E 56 41 53</div><div>_OpenVAS</div></div></div>
<div>Impact</div> <div>An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.</div>
<div>Solution:</div> <div>Solution type: VendorFix</div> <div>Updates are available. Please see the referenced vendor advisory.</div>
<div>Affected Software/OS</div> <div>This issue affects Samba 3.0.0 through 3.0.25rc3.</div>
<div>Vulnerability Detection Method</div> <div>Sends a crafted SMB request and checks if the target is connecting back to the scanner host.</div> <div>Note: For a successful detection of this flaw the scanner host needs to be able to directly receive ICMP echo requests from the target.</div> <div>Details: Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check</div> <div>OID:1.3.6.1.4.1.25623.1.0.108011</div> <div>Version used: 2024-11-13T05:05:39Z</div>
<div>Product Detection Result</div> <div>... continues on next page ...</div>

...continued from previous page ...
Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
<b>References</b> cve: CVE-2007-2447 url: <a href="http://www.securityfocus.com/bid/23972">http://www.securityfocus.com/bid/23972</a> url: <a href="https://www.samba.org/samba/security/CVE-2007-2447.html">https://www.samba.org/samba/security/CVE-2007-2447.html</a>

[\[ return to 10.0.2.5 \]](#)

### 2.1.22 Medium 2121/tcp

Medium (CVSS: 4.8) NVT: FTP Unencrypted Cleartext Login
<b>Summary</b> The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↔. Response(s): Non-anonymous sessions: 331 Password required for openvasvt Anonymous sessions: 331 Password required for anonymous
<b>Impact</b> An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
<b>Solution:</b> <b>Solution type:</b> Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
<b>Vulnerability Detection Method</b> Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108528
... continues on next page ...

...continued from previous page...

Version used: 2023-12-20T05:05:58Z

[\[ return to 10.0.2.5 \]](#)**2.1.23 Medium 5900/tcp**

Medium (CVSS: 4.8)

NVT: VNC Server Unencrypted Data Transmission

**Summary**

The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.

**Quality of Detection (QoD):** 70%**Vulnerability Detection Result**

The VNC server provides the following insecure or cryptographically weak Security Type(s):  
2 (VNC authentication)

**Impact**

An attacker can uncover sensitive data by sniffing traffic to the VNC server.

**Solution:****Solution type:** Mitigation

Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.

**Vulnerability Detection Method**

Details: VNC Server Unencrypted Data Transmission

OID:1.3.6.1.4.1.25623.1.0.108529

Version used: 2023-07-12T05:05:04Z

**References**url: <https://tools.ietf.org/html/rfc6143#page-10>[\[ return to 10.0.2.5 \]](#)**2.1.24 Medium 21/tcp**

Medium (CVSS: 6.4)
NVT: Anonymous FTP Login Reporting
<b>Summary</b> Reports if the remote FTP Server allows anonymous logins.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was possible to login to the remote FTP service with the following anonymous ↪account(s): anonymous:anonymous@example.com ftp:anonymous@example.com
<b>Impact</b> Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to: - gain access to sensitive files - upload or delete files.
<b>Solution:</b> <b>Solution type:</b> Mitigation If you do not want to share files, you should disable anonymous logins.
<b>Vulnerability Insight</b> A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data. Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.
<b>Vulnerability Detection Method</b> Details: Anonymous FTP Login Reporting OID:1.3.6.1.4.1.25623.1.0.900600 Version used: 2021-10-20T09:03:29Z
<b>References</b> cve: CVE-1999-0497

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login
<b>Summary</b> The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↪. Response(s): Non-anonymous sessions: 331 Please specify the password. Anonymous sessions: 331 Please specify the password.
<b>Impact</b> An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
<b>Solution:</b> <b>Solution type:</b> Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
<b>Vulnerability Detection Method</b> Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108528 Version used: 2023-12-20T05:05:58Z

[\[ return to 10.0.2.5 \]](#)

### 2.1.25 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
<b>Product detection result</b> cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)
... continues on next page ...

... continued from previous page ...

Summary

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

The remote SSH server supports the following weak KEX algorithm(s):

KEX algorithm	Reason
-----	
↪-----	
diffie-hellman-group-exchange-sha1	Using SHA-1
diffie-hellman-group1-sha1	Using Oakley Group 2 (a 1024-bit MODP group ↪) and SHA-1

Impact

An attacker can quickly break individual connections.

Solution:

Solution type: Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight

- 1024-bit MODP group / prime KEX algorithms:

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.

A nation-state can break a 1024-bit prime.

Vulnerability Detection Method

Checks the supported KEX algorithms of the remote SSH server.

Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime

- ephemeraly generated key exchange groups uses SHA-1

- using RSA 1024-bit modulus key

Details: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

OID:1.3.6.1.4.1.25623.1.0.150713

Version used: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:secure\_shell\_protocol

Method: SSH Protocol Algorithms Supported

... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.105565)
<b>References</b> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a> url: <a href="https://www.rfc-editor.org/rfc/rfc9142">https://www.rfc-editor.org/rfc/rfc9142</a> url: <a href="https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implementations">https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implementations</a> url: <a href="https://www.rfc-editor.org/rfc/rfc6194">https://www.rfc-editor.org/rfc/rfc6194</a> url: <a href="https://www.rfc-editor.org/rfc/rfc4253#section-6.5">https://www.rfc-editor.org/rfc/rfc4253#section-6.5</a>
<b>Medium (CVSS: 5.3)</b> <b>NVT: Weak Host Key Algorithm(s) (SSH)</b>
<b>Product detection result</b> cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)
<b>Summary</b> The remote SSH server is configured to allow / support weak host key algorithm(s).
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> The remote SSH server supports the following weak host key algorithm(s): host key algorithm   Description ----- ↪----- ssh-dss   Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS) ↪
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the reported weak host key algorithm(s).
<b>Vulnerability Detection Method</b> Checks the supported host key algorithms of the remote SSH server. Currently weak host key algorithms are defined as the following: - ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS) Details: Weak Host Key Algorithm(s) (SSH) OID:1.3.6.1.4.1.25623.1.0.117687 Version used: 2024-06-14T05:05:48Z
... continues on next page ...



...continued from previous page ...
<b>Product Detection Result</b> Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)
<b>References</b> url: <a href="https://www.rfc-editor.org/rfc/rfc8332">https://www.rfc-editor.org/rfc/rfc8332</a> url: <a href="https://www.rfc-editor.org/rfc/rfc8709">https://www.rfc-editor.org/rfc/rfc8709</a> url: <a href="https://www.rfc-editor.org/rfc/rfc4253#section-6.6">https://www.rfc-editor.org/rfc/rfc4253#section-6.6</a>

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)
<b>Product detection result</b> cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)
<b>Summary</b> The remote SSH server is configured to allow / support weak encryption algorithm(s).
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> The remote SSH server supports the following weak client-to-server encryption al ↪gorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se The remote SSH server supports the following weak server-to-client encryption al ↪gorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour
... continues on next page ...

...continued from previous page...	
<pre>arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se</pre>	
<b>Solution:</b>	
<b>Solution type:</b> Mitigation	
Disable the reported weak encryption algorithm(s).	
<b>Vulnerability Insight</b>	
<ul style="list-style-type: none"> <li>- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.</li> <li>- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.</li> <li>- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.</li> </ul>	
<b>Vulnerability Detection Method</b>	
<p>Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.</p> <p>Currently weak encryption algorithms are defined as the following:</p> <ul style="list-style-type: none"> <li>- Arcfour (RC4) cipher based algorithms</li> <li>- 'none' algorithm</li> <li>- CBC mode cipher based algorithms</li> </ul> <p>Details: Weak Encryption Algorithm(s) Supported (SSH)</p> <p>OID:1.3.6.1.4.1.25623.1.0.105611</p> <p>Version used: 2024-06-14T05:05:48Z</p>	
<b>Product Detection Result</b>	
<p>Product: cpe:/a:ietf:secure_shell_protocol</p> <p>Method: SSH Protocol Algorithms Supported</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105565)</p>	
<b>References</b>	
<p>url: <a href="https://www.rfc-editor.org/rfc/rfc8758">https://www.rfc-editor.org/rfc/rfc8758</a></p> <p>url: <a href="https://www.kb.cert.org/vuls/id/958563">https://www.kb.cert.org/vuls/id/958563</a></p> <p>url: <a href="https://www.rfc-editor.org/rfc/rfc4253#section-6.3">https://www.rfc-editor.org/rfc/rfc4253#section-6.3</a></p>	

[\[ return to 10.0.2.5 \]](#)

### 2.1.26 Low 25/tcp

Low (CVSS: 3.7)
NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)
<b>Product detection result</b> cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↪802067)
<b>Summary</b> This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> 'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
<b>Impact</b> Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.
<b>Solution:</b> <b>Solution type:</b> VendorFix - Remove support for 'DHE_EXPORT' cipher suites from the service - If running OpenSSL update to version 1.0.2b or 1.0.1n or later.
<b>Affected Software/OS</b> - Hosts accepting 'DHE_EXPORT' cipher suites - OpenSSL version before 1.0.2b and 1.0.1n
<b>Vulnerability Insight</b> Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.
<b>Vulnerability Detection Method</b> Check previous collected cipher suites saved in the KB. Details: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.805188 Version used: 2024-09-30T08:38:05Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)
<b>References</b> cve: CVE-2015-4000 url: <a href="https://weakdh.org">https://weakdh.org</a> url: <a href="http://www.securityfocus.com/bid/74733">http://www.securityfocus.com/bid/74733</a> url: <a href="https://weakdh.org/imperfect-forward-secrecy.pdf">https://weakdh.org/imperfect-forward-secrecy.pdf</a> url: <a href="http://openwall.com/lists/oss-security/2015/05/20/8">http://openwall.com/lists/oss-security/2015/05/20/8</a> url: <a href="https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained">https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained</a> url: <a href="https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes">https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes</a> cert-bund: CB-K21/0067 cert-bund: CB-K19/0812 cert-bund: CB-K16/1593 cert-bund: CB-K16/1552 cert-bund: CB-K16/0617 cert-bund: CB-K16/0599 cert-bund: CB-K16/0168 cert-bund: CB-K16/0121 cert-bund: CB-K16/0090 cert-bund: CB-K16/0030 cert-bund: CB-K15/1591 cert-bund: CB-K15/1550 cert-bund: CB-K15/1517 cert-bund: CB-K15/1464 cert-bund: CB-K15/1442 cert-bund: CB-K15/1334 cert-bund: CB-K15/1269 cert-bund: CB-K15/1136 cert-bund: CB-K15/1090 cert-bund: CB-K15/1059 cert-bund: CB-K15/1022 cert-bund: CB-K15/1015 cert-bund: CB-K15/0964 cert-bund: CB-K15/0932 cert-bund: CB-K15/0927 cert-bund: CB-K15/0926 cert-bund: CB-K15/0907 cert-bund: CB-K15/0901 cert-bund: CB-K15/0896 cert-bund: CB-K15/0877
...continues on next page ...

...continued from previous page ...

```

cert-bund: CB-K15/0834
cert-bund: CB-K15/0802
cert-bund: CB-K15/0733
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0737

```

Low (CVSS: 3.4)

NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**

cpe:/a:ietf:transport\_layer\_security

...continues on next page ...

...continued from previous page ...
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↪802067)
<b>Summary</b> This host is prone to an information disclosure vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
<b>Solution:</b> <b>Solution type:</b> Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
<b>Vulnerability Insight</b> The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
<b>Vulnerability Detection Method</b> Evaluate previous collected information about this service. Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↪.. OID:1.3.6.1.4.1.25623.1.0.802087 Version used: 2024-09-30T08:38:05Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)
<b>References</b> cve: CVE-2014-3566 url: <a href="https://www.openssl.org/~bodo/ssl-poodle.pdf">https://www.openssl.org/~bodo/ssl-poodle.pdf</a> url: <a href="http://www.securityfocus.com/bid/70574">http://www.securityfocus.com/bid/70574</a> url: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a> 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>
... continues on next page ...

...continued from previous page ...

```

url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin
↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468

```

...continues on next page ...

...continued from previous page ...	
dfn-cert:	DFN-CERT-2016-1168
dfn-cert:	DFN-CERT-2016-0884
dfn-cert:	DFN-CERT-2016-0642
dfn-cert:	DFN-CERT-2016-0388
dfn-cert:	DFN-CERT-2016-0171
dfn-cert:	DFN-CERT-2015-1431
dfn-cert:	DFN-CERT-2015-1075
dfn-cert:	DFN-CERT-2015-1026
dfn-cert:	DFN-CERT-2015-0664
dfn-cert:	DFN-CERT-2015-0548
dfn-cert:	DFN-CERT-2015-0404
dfn-cert:	DFN-CERT-2015-0396
dfn-cert:	DFN-CERT-2015-0259
dfn-cert:	DFN-CERT-2015-0254
dfn-cert:	DFN-CERT-2015-0245
dfn-cert:	DFN-CERT-2015-0118
dfn-cert:	DFN-CERT-2015-0114
dfn-cert:	DFN-CERT-2015-0083
dfn-cert:	DFN-CERT-2015-0082
dfn-cert:	DFN-CERT-2015-0081
dfn-cert:	DFN-CERT-2015-0076
dfn-cert:	DFN-CERT-2014-1717
dfn-cert:	DFN-CERT-2014-1680
dfn-cert:	DFN-CERT-2014-1632
dfn-cert:	DFN-CERT-2014-1564
dfn-cert:	DFN-CERT-2014-1542
dfn-cert:	DFN-CERT-2014-1414
dfn-cert:	DFN-CERT-2014-1366
dfn-cert:	DFN-CERT-2014-1354

[\[ return to 10.0.2.5 \]](#)

2.1.27 Low 5432/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
<b>Product detection result</b> cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↪802067)
... continues on next page ...



...continued from previous page ...
<b>Summary</b> This host is prone to an information disclosure vulnerability.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
<b>Solution:</b> <b>Solution type:</b> Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
<b>Vulnerability Insight</b> The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
<b>Vulnerability Detection Method</b> Evaluate previous collected information about this service. Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↔.. OID:1.3.6.1.4.1.25623.1.0.802087 Version used: 2024-09-30T08:38:05Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)
<b>References</b> cve: CVE-2014-3566 url: <a href="https://www.openssl.org/~bodo/ssl-poodle.pdf">https://www.openssl.org/~bodo/ssl-poodle.pdf</a> url: <a href="http://www.securityfocus.com/bid/70574">http://www.securityfocus.com/bid/70574</a> url: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a> 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> url: <a href="http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin">http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin</a> ↔g-ssl-30.html cert-bund: WID-SEC-2023-0431 cert-bund: CB-K17/1198
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K17/1196  
cert-bund: CB-K16/1828  
cert-bund: CB-K16/1438  
cert-bund: CB-K16/1384  
cert-bund: CB-K16/1102  
cert-bund: CB-K16/0599  
cert-bund: CB-K16/0156  
cert-bund: CB-K15/1514  
cert-bund: CB-K15/1358  
cert-bund: CB-K15/1021  
cert-bund: CB-K15/0972  
cert-bund: CB-K15/0637  
cert-bund: CB-K15/0590  
cert-bund: CB-K15/0525  
cert-bund: CB-K15/0393  
cert-bund: CB-K15/0384  
cert-bund: CB-K15/0287  
cert-bund: CB-K15/0252  
cert-bund: CB-K15/0246  
cert-bund: CB-K15/0237  
cert-bund: CB-K15/0118  
cert-bund: CB-K15/0110  
cert-bund: CB-K15/0108  
cert-bund: CB-K15/0080  
cert-bund: CB-K15/0078  
cert-bund: CB-K15/0077  
cert-bund: CB-K15/0075  
cert-bund: CB-K14/1617  
cert-bund: CB-K14/1581  
cert-bund: CB-K14/1537  
cert-bund: CB-K14/1479  
cert-bund: CB-K14/1458  
cert-bund: CB-K14/1342  
cert-bund: CB-K14/1314  
cert-bund: CB-K14/1313  
cert-bund: CB-K14/1311  
cert-bund: CB-K14/1304  
cert-bund: CB-K14/1296  
dfn-cert: DFN-CERT-2017-1238  
dfn-cert: DFN-CERT-2017-1236  
dfn-cert: DFN-CERT-2016-1929  
dfn-cert: DFN-CERT-2016-1527  
dfn-cert: DFN-CERT-2016-1468  
dfn-cert: DFN-CERT-2016-1168  
dfn-cert: DFN-CERT-2016-0884  
dfn-cert: DFN-CERT-2016-0642  
dfn-cert: DFN-CERT-2016-0388

...continues on next page ...

...continued from previous page ...	
dfn-cert:	DFN-CERT-2016-0171
dfn-cert:	DFN-CERT-2015-1431
dfn-cert:	DFN-CERT-2015-1075
dfn-cert:	DFN-CERT-2015-1026
dfn-cert:	DFN-CERT-2015-0664
dfn-cert:	DFN-CERT-2015-0548
dfn-cert:	DFN-CERT-2015-0404
dfn-cert:	DFN-CERT-2015-0396
dfn-cert:	DFN-CERT-2015-0259
dfn-cert:	DFN-CERT-2015-0254
dfn-cert:	DFN-CERT-2015-0245
dfn-cert:	DFN-CERT-2015-0118
dfn-cert:	DFN-CERT-2015-0114
dfn-cert:	DFN-CERT-2015-0083
dfn-cert:	DFN-CERT-2015-0082
dfn-cert:	DFN-CERT-2015-0081
dfn-cert:	DFN-CERT-2015-0076
dfn-cert:	DFN-CERT-2014-1717
dfn-cert:	DFN-CERT-2014-1680
dfn-cert:	DFN-CERT-2014-1632
dfn-cert:	DFN-CERT-2014-1564
dfn-cert:	DFN-CERT-2014-1542
dfn-cert:	DFN-CERT-2014-1414
dfn-cert:	DFN-CERT-2014-1366
dfn-cert:	DFN-CERT-2014-1354

[\[ return to 10.0.2.5 \]](#)

### 2.1.28 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 581004 Packet 2: 581111
... continues on next page ...

...continued from previous page...	
<b>Impact</b>	A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b>	
<b>Solution type:</b> Mitigation	
<p>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.</p> <p>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.</p> <p>See the references for more information.</p>	
<b>Affected Software/OS</b>	TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b>	The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b>	<p>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.</p> <p>Details: TCP Timestamps Information Disclosure</p> <p>OID:1.3.6.1.4.1.25623.1.0.80091</p> <p>Version used: 2023-12-15T16:10:08Z</p>
<b>References</b>	<p>url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a></p> <p>url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a></p> <p>url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a></p>

[\[ return to 10.0.2.5 \]](#)

### 2.1.29 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
<b>Product detection result</b>
cpe:/a:ietf:secure_shell_protocol
...continues on next page...

...continued from previous page ...
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↔)
<b>Summary</b> The remote SSH server is configured to allow / support weak MAC algorithm(s).
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> The remote SSH server supports the following weak client-to-server MAC algorithm ↔(s): hmac-md5 hmac-md5-96 hmac-sha1-96 umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↔(s): hmac-md5 hmac-md5-96 hmac-sha1-96 umac-64@openssh.com
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the reported weak MAC algorithm(s).
<b>Vulnerability Detection Method</b> Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2024-06-14T05:05:48Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)
<b>References</b>
... continues on next page ...

...continued from previous page ...

url: <https://www.rfc-editor.org/rfc/rfc6668>url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.4>[\[ return to 10.0.2.5 \]](#)**2.1.30 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

**Quality of Detection (QoD):** 80%**Vulnerability Detection Result**

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:****Solution type:** Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2023-05-11T09:09:33Z

... continues on next page ...

...continued from previous page ...

**References**

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>

url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 10.0.2.5 \]](#)

---

This file was automatically generated.