

Scan Report

February 10, 2026

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 “Metasploitable 192.168.186.129 Week4 Remediation scan Clone 2”. The scan started at Tue Feb 10 08:07:49 2026 UTC and ended at Tue Feb 10 08:32:33 2026 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1	Result Overview	2
1.1	Host Authentications	2
2	Results per Host	2
2.1	192.168.186.129	2
2.1.1	Critical 80/tcp	3
2.1.2	Critical 8787/tcp	6
2.1.3	Critical 8009/tcp	8
2.1.4	Critical 5900/tcp	14
2.1.5	Critical general/tcp	15
2.1.6	Critical 3632/tcp	16
2.1.7	Critical 5432/tcp	17
2.1.8	Critical 3306/tcp	18
2.1.9	High 80/tcp	19
2.1.10	High 2121/tcp	21
2.1.11	High 6697/tcp	23
2.1.12	High 1099/tcp	25
2.1.13	High 5432/tcp	27
2.1.14	Medium 80/tcp	29
2.1.15	Medium 2121/tcp	43
2.1.16	Medium 5900/tcp	44

CONTENTS	2
----------	---

2.1.17 Medium 22/tcp	45
2.1.18 Medium 445/tcp	49
2.1.19 Medium 25/tcp	50
2.1.20 Medium 5432/tcp	69
2.1.21 Low general/icmp	87
2.1.22 Low general/tcp	88
2.1.23 Low 22/tcp	89
2.1.24 Low 25/tcp	91
2.1.25 Low 5432/tcp	97

1 Result Overview

Host	Critical	High	Medium	Low	Log	False P.
192.168.186.129	9	7	37	6	0	0
Total: 1	9	7	37	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 59 results selected by the filtering described above. Before filtering there were 611 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.186.129	SSH	Failure	Protocol SSH, Port 22, User msfadmin : Login failure
192.168.186.129	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.186.129

Host scan start Tue Feb 10 08:08:52 2026 UTC

Host scan end Tue Feb 10 08:32:30 2026 UTC

Service (Port)	Threat Level
80/tcp	Critical
8787/tcp	Critical
8009/tcp	Critical
5900/tcp	Critical
general/tcp	Critical
3632/tcp	Critical
5432/tcp	Critical
3306/tcp	Critical

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
80/tcp	High
2121/tcp	High
6697/tcp	High
1099/tcp	High
5432/tcp	High
80/tcp	Medium
2121/tcp	Medium
5900/tcp	Medium
22/tcp	Medium
445/tcp	Medium
25/tcp	Medium
5432/tcp	Medium
general/icmp	Low
general/tcp	Low
22/tcp	Low
25/tcp	Low
5432/tcp	Low

2.1.1 Critical 80/tcp

Critical (CVSS: 10.0)
NVT: TWiki < 4.2.4 Multiple XSS / Command Execution Vulnerabilities
Summary TWiki is prone to multiple cross-site scripting (XSS) and command execution vulnerabilities.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 4.2.4
Impact Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.
Solution: Solution type: VendorFix Update to version 4.2.4 or later.
Affected Software/OS ... continues on next page ...

	... continued from previous page ...
TWiki versions prior to 4.2.4.	
Vulnerability Insight	
The flaws are due to:	
- %URLPARAM}}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.	
- %SEARCH}}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.	
Vulnerability Detection Method	
Details: TWiki < 4.2.4 Multiple XSS / Command Execution Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.800320 Version used: 2025-12-11T05:46:19Z	
References	
cve: CVE-2008-5304	
cve: CVE-2008-5305	
url: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304	
url: http://www.securityfocus.com/bid/32668	
url: http://www.securityfocus.com/bid/32669	
url: http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305	

Critical (CVSS: 9.8)
NVT: PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check
Summary
PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 95%
Vulnerability Detection Result
By doing the following HTTP POST request: <pre>"HTTP POST" body : <?php phpinfo();?> URL : http://192.168.186.129/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%3 ↪D%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%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%2 ↪E%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.</pre>
Result:
<pre><title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX, NOFOLLOW, NOARCHIV ↪E" /></head></pre>
... continues on next page ...

<p>... continued from previous page ...</p> <pre><tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph →p5/cgi </td></tr> <h2>PHP Core</h2> <h2>PHP Variables</h2></pre> <p>Impact Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.</p> <p>Solution: Solution type: VendorFix PHP: Update to version 5.3.13, 5.4.3 or later - Other products / applications: Please contact the vendor for a solution</p> <p>Affected Software/OS PHP versions prior to 5.3.13 and 5.4.x prior to 5.4.3. Other products / applications might be affected by the tested CVE-2012-1823 as well.</p> <p>Vulnerability Insight When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution. An example of the -s command, allowing an attacker to view the source code of index.php is below: http://example.com/index.php?-s</p> <p>Vulnerability Detection Method Send multiple crafted HTTP POST requests and checks the responses. Notes: - This script checks for the presence of CVE-2012-1823 which indicates that the system is also affected by the other included CVES. - It is currently expected that a result of this VT is reported if the system is generally exposing a phpinfo() output on the relevant URL / endpoint (independent from the running product). Exposing such sensitive information is generally seen as a security misconfiguration and should be avoided. Details: PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check OID:1.3.6.1.4.1.25623.1.0.103482 Version used: 2025-11-11T05:40:18Z</p> <p>References cve: CVE-2012-1823 cve: CVE-2012-2311 cve: CVE-2012-2336 cve: CVE-2012-2335</p>
... continues on next page ...

... continued from previous page ...

```
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
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
```

[[return to 192.168.186.129](#)]

2.1.2 Critical 8787/tcp

Critical (CVSS: 10.0)

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

Summary

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

Quality of Detection (QoD): 99%

... continues on next page ...

<p>... continued from previous page ...</p>

Vulnerability Detection Result

The service is running in `$SAFE >= 1` mode. However it is still possible to run arbitrary syscall commands on the remote host. Sending an invalid syscall the service returned the following response:

```
Flo::Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/druby.rb:1555:in `syscall'"0/usr/lib/ruby/1.8/druby.rb:1555:in `send'"4/usr/lib/ruby/1.8/druby.rb:1555:in `__send__'"A/usr/lib/ruby/1.8/druby.rb:1555:in `perform_without_block'"3/usr/lib/ruby/1.8/druby.rb:1515:in `perform'"5/usr/lib/ruby/1.8/druby.rb:1589:in `main_loop'"0/usr/lib/ruby/1.8/druby.rb:1585:in `loop'"5/usr/lib/ruby/1.8/druby.rb:1585:in `main_loop'"1/usr/lib/ruby/1.8/druby.rb:1581:in `start'"5/usr/lib/ruby/1.8/druby.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/druby.rb:143<0:in `run'"1/usr/lib/ruby/1.8/druby.rb:1427:in `start'"//usr/lib/ruby/1.8/druby.rb:1427:in `run'"6/usr/lib/ruby/1.8/druby.rb:1347:in `initialize'"//usr/lib/ruby/1.8/druby.rb:1627:in `new'"9/usr/lib/ruby/1.8/druby.rb:1627:in `start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not implemented
```

Impact

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

Solution:

Solution type: Mitigation

Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:

- Implementing taint on untrusted input
- Setting `$SAFE` levels appropriately ($>=2$ is recommended if untrusted hosts are allowed to submit Ruby commands, and $>=3$ may be appropriate)
- Including `drb/acl.rb` to set ACLEntry to restrict access to trusted hosts

Vulnerability Detection Method

Send a crafted command to the service and check for a remote command execution via the `instance_eval` or `syscall` requests.

Details: **Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities**

OID:1.3.6.1.4.1.25623.1.0.108010

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

References

- url: <https://tools.cisco.com/security/center/viewAlert.x?alertId=22750>
- url: <http://www.securityfocus.com/bid/47071>
- url: http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testers/

... continues on next page ...

	... continued from previous page ...
	url: http://www.ruby-doc.org/stdlib-1.9.3/libdoc/druby/rdoc/DRb.html

[return to 192.168.186.129]

2.1.3 Critical 8009/tcp

Critical (CVSS: 9.8)
NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check
Summary Apache Tomcat is prone to a remote code execution (RCE) vulnerability in the AJP connector dubbed 'Ghostcat'.
Quality of Detection (QoD): 99%
<p>Vulnerability Detection Result It was possible to read the file "/WEB-INF/web.xml" through the AJP connector. Result: AB 8\x0004 \x0088 \x00020K \x0001 \x000CContent-Type \x001Ctext/html;charset=→ISO-8859-1 AB\x001F\x003\x001F,<!-- Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to You under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. --> <?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "mailto:http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"> <head> <title>Apache Tomcat/5.5</title> <style type="text/css"> /*<![CDATA[*/ body { color: #000000; background-color: #FFFFFF;</p>

... continues on next page ...

... continued from previous page ...

```
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;
}

#banner {
    margin-bottom: 12px;
}
p#congrats {
    margin-top: 0;
    font-weight: bold;
    text-align: center;
}
p#footer {
    text-align: right;
    font-size: 80%;
```

... continues on next page ...

... continued from previous page ...

```
    }
    /*]]>/*
</style>
</head>
<body>
<!-- Header --&gt;
&lt;table id="banner" width="100%"&gt;
    &lt;tr&gt;
        &lt;td align="left" style="width:130px"&gt;
            &lt;a href="http://tomcat.apache.org/"&gt;
                &lt;img src="tomcat.gif" height="92" width="130" alt="The Mighty Tomcat - MEOW!"/&gt;
            &lt;/a&gt;
        &lt;/td&gt;
        &lt;td align="left" valign="top"&gt;&lt;b&gt;Apache Tomcat/5.5&lt;/b&gt;&lt;/td&gt;
        &lt;td align="right"&gt;
            &lt;a href="http://www.apache.org/"&gt;
                &lt;img src="ASF-Logo-Wide.gif" height="51" width="537" alt="The Apache Software
→ Foundation"/&gt;
            &lt;/a&gt;
        &lt;/td&gt;
    &lt;/tr&gt;
&lt;/table&gt;
&lt;table&gt;
    &lt;tr&gt;
        &lt;!-- Table of Contents --&gt;
        &lt;td valign="top"&gt;
            &lt;table width="100%" border="1" cellspacing="0" cellpadding="3"&gt;
                &lt;tr&gt;
                    &lt;th&gt;Administration&lt;/th&gt;
                &lt;/tr&gt;
                &lt;tr&gt;
                    &lt;td class="menu"&gt;
                        &lt;a href="manager/status"&gt;Status&lt;/a&gt;&lt;br /&gt;
                            &lt;a href="admin"&gt;Tomcat&amp;nbsp;Administration&lt;/a&gt;&lt;br /&gt;
                            &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;</pre>
```

... continues on next page ...

<code> ... continued from previous page ... Release &nbsp;Notes
 Change &nbsp;Log
 ↵> ↵ Tomcat &nbsp;Documentation
 ↵ &nbsp; &nbsp; </code>
<code> </td> </tr> </table>
 <table width="100%" border="1" cellspacing="0" cellpadding="3"> <tr> <th>Tomcat Online</th> </tr> <tr> <td class="menu"> Home &nbsp;Page
 FAQ
 Bug &nbsp;D ↵atabase
 Open Bugs
 Users &nbsp;Mailing &nbsp;List
 Developers &nbsp;Mailing &nbsp;List
 IRC
 &nbsp; </td> </tr> </table>
 <table width="100%" border="1" cellspacing="0" cellpadding="3"> <tr> <th>Examples</th> </tr> <tr> <td class="menu"> JSP &nbsp;Examples
 Servlet &nbsp;Examples
 WebDAV &nbsp;capabilities
 &nbsp; </td> </tr> </code>

... continues on next page ...

... continued from previous page ...

```

        </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 Java&n
→bsp;Server&ampnbspPages&ampnbspSite</a><br/>
            <a href="http://java.sun.com/products/servlet">Sun's Se
→rvlet&ampnbspSite</a><br/>
            &ampnbsp
        </td>
    </tr>
</table>
</td>
<td style="width:20px">&ampnbsp</td>

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

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

    <p>where "$CATALINA_HOME" is the root of the Tomcat installation direc
→tory. If you're seeing this page, and you don't think you should be, then eith
→er you're either a user who has arrived at new installation of Tomcat, or you'
→re an administrator who hasn't got his/her setup quite right. Providing the la
→tter is the case, please refer to the <a href="tomcat-docs">Tomcat Documentati
→on</a> for more detailed setup and administration information than is found in
→ the INSTALL file.</p>
    <p><b>NOTE:</b> This page is precompiled. If you change it, this pag
→e will not change since
        it was compiled into a servlet at build time.
        (See <tt>$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml</tt> as t
→o how it was mapped.)
    </p>
    <p><b>NOTE:</b> For security reasons, using the administration webapp
        is restricted to users with role "admin". The manager webapp
        is restricted to users with role "manager".</b>

```

... continues on next page ...

<p>... continued from previous page ...</p> <pre> Users are defined in <code>\$CATALINA_HOME/conf/tomcat-users.xml</code> </pre>.</p> <p>Included with this release are a host of sample Servlets and JSPs → (with associated source code), extensive documentation (including the Servlet → 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web app →lications.</p> <p>Tomcat mailing lists are available at the Tomcat project web site →:</p> users@tomc </pre>
<p>Solution:</p> <p>Solution type: VendorFix</p> <ul style="list-style-type: none"> - 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
<p>Affected Software/OS</p> <p>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.</p>
<p>Vulnerability Insight</p> <p>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.</p>
<p>Vulnerability Detection Method</p> <p>Sends a crafted AJP request and checks the response.</p> <p>Details: Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check OID:1.3.6.1.4.1.25623.1.0.143545 Version used: 2025-07-11T05:42:17Z</p>
<p>References</p> <p>cve: CVE-2020-1938 url: https://lists.apache.org/thread/bnys51vg1875dsslkkx2vmwxv833135x url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.31 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.51 url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.100 url: https://web.archive.org/web/20250114042903/https://www.chaitin.cn/en/ghostcat-at url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487 url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/ url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog cisa: Known Exploited Vulnerability (KEV) catalog</p>
... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2023-2480
cert-bund: CB-K20/0711
cert-bund: CB-K20/0705
cert-bund: CB-K20/0693
cert-bund: CB-K20/0555
cert-bund: CB-K20/0543
cert-bund: CB-K20/0154
dfn-cert: DFN-CERT-2021-1736
dfn-cert: DFN-CERT-2020-1508
dfn-cert: DFN-CERT-2020-1413
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2020-1134
dfn-cert: DFN-CERT-2020-0850
dfn-cert: DFN-CERT-2020-0835
dfn-cert: DFN-CERT-2020-0821
dfn-cert: DFN-CERT-2020-0569
dfn-cert: DFN-CERT-2020-0557
dfn-cert: DFN-CERT-2020-0501
dfn-cert: DFN-CERT-2020-0381
```

[[return to 192.168.186.129](#)]

2.1.4 Critical 5900/tcp

Critical (CVSS: 9.0)

NVT: VNC Brute Force Login

Summary

Try to log in with given passwords via VNC protocol.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

It was possible to connect to the VNC server with the password: password

Solution:

Solution type: Mitigation

Change the password to something hard to guess or enable password protection at all.

Vulnerability Insight

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.

... continues on next page ...

<p>... continued from previous page ...</p> <p>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.</p> <p>Note as well that passwords can be max. 8 characters long.</p>

<p>Vulnerability Detection Method</p> <p>Details: VNC Brute Force Login OID:1.3.6.1.4.1.25623.1.0.106056 Version used: 2021-07-23T07:56:26Z</p>

[[return to 192.168.186.129](#)]

2.1.5 Critical general/tcp

<p>Critical (CVSS: 10.0)</p>

<p>NVT: Operating System (OS) End of Life (EOL) Detection</p>

Product detection result

<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>

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

<p>The "Ubuntu" Operating System on the remote host has reached the end of life. CPE: cpe:/o:canonical:ubuntu_linux:8.04 Installed version, build or SP: 8.04 EOL date: 2013-05-09 EOL info: https://documentation.ubuntu.com/project/release-team/list-of-releases/</p>

Impact

<p>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.</p>

Solution:

<p>Solution type: Mitigation</p>

<p>... continues on next page ...</p>

<p>... continued from previous page ...</p> <p>Update the OS on the remote host to a version which is still supported and receiving security updates by the vendor.</p> <p>Note / Important: Please create an override for this result if the target host is a:</p> <ul style="list-style-type: none"> - Windows system with Extended Security Updates (ESU) - System with additional 3rd-party / non-vendor security updates like e.g. from 'TuxCare', 'Freexian Extended LTS' or similar
<p>Vulnerability Detection Method</p> <p>Checks if an EOL version of an OS is present on the target host.</p> <p>Details: Operating System (OS) End of Life (EOL) Detection OID:1.3.6.1.4.1.25623.1.0.103674 Version used: 2025-05-21T05:40:19Z</p>
<p>Product Detection Result</p> <p>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)</p>

[[return to 192.168.186.129](#)]

2.1.6 Critical 3632/tcp

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

... continued from previous page ...

Vulnerability Insight

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

Vulnerability Detection Method

Details: DistCC RCE Vulnerability (CVE-2004-2687)

OID: 1.3.6.1.4.1.25623.1.0.103553

Version used: 2022-07-07T10:16:06Z

References

cve: CVE-2004-2687

url: <https://distcc.github.io/security.html>

url: <https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80%2Farchives/bugtraq/2005-03/0183.html>

dfn-cert: DFN-CERT-2019-0381

[[return to 192.168.186.129](#)]

2.1.7 Critical 5432/tcp

Critical (CVSS: 9.0)

NVT: PostgreSQL Default Credentials (PostgreSQL Protocol)

Product detection result

cpe:/a:postgresql:postgresql:8.3.1

Detected by PostgreSQL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.12802
→5)

Summary

It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

It was possible to login as user postgres with password "postgres".

Solution:

Solution type: Mitigation

Change the password as soon as possible.

... continues on next page ...

Vulnerability Detection Method Details: PostgreSQL Default Credentials (PostgreSQL Protocol) OID: 1.3.6.1.4.1.25623.1.0.103552 Version used: 2024-07-19T15:39:06Z	... continued from previous page ...
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------

Product Detection Result

Product: cpe:/a:postgresql:postgresql:8.3.1
 Method: PostgreSQL Detection Consolidation
 OID: 1.3.6.1.4.1.25623.1.0.128025)

[[return to 192.168.186.129](#)]

2.1.8 Critical 3306/tcp

Critical (CVSS: 9.8)

NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)

Product detection result

cpe:/a:mysql:mysql:5.0.51a
 Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.25623.1.0.100152)

Summary

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

Quality of Detection (QoD): 95%
Vulnerability Detection Result

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

Solution:

Solution type: Mitigation

- Change the password as soon as possible
- Contact the vendor for other possible fixes / updates

Affected Software/OS

The following products are known to use such weak credentials:

- CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x
- CVE-2002-1809: Windows binary release of MySQL 3.23.2 through 3.23.52
- CVE-2004-1532: AppServ 2.5.x and earlier
- CVE-2004-2357: Proofpoint Protection Server
- CVE-2006-1451: MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6

... continues on next page ...

... continued from previous page ...
- CVE-2007-2554: Associated Press (AP) Newswire 4.0.1 and earlier - CVE-2007-6081: AdventNet EventLog Analyzer build 4030 - CVE-2009-0919: XAMPP - CVE-2014-3419: Infoblox NetMRI before 6.8.5 - CVE-2015-4669: Xsuite 2.x - CVE-2016-6531, CVE-2018-15719: Open Dental before version 18.4 - CVE-2024-22901: Vinchin Backup & Recovery 7.2 and prior Other products might be affected as well.
Vulnerability Detection Method Details: MySQL / MariaDB Default Credentials (MySQL Protocol) OID: 1.3.6.1.4.1.25623.1.0.103551 Version used: 2025-09-09T05:38:49Z
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MariaDB / Oracle MySQL Detection (MySQL Protocol) OID: 1.3.6.1.4.1.25623.1.0.100152)
References cve: CVE-2001-0645 cve: CVE-2002-1809 cve: CVE-2004-1532 cve: CVE-2004-2357 cve: CVE-2006-1451 cve: CVE-2007-2554 cve: CVE-2007-6081 cve: CVE-2009-0919 cve: CVE-2014-3419 cve: CVE-2015-4669 cve: CVE-2016-6531 cve: CVE-2018-15719 cve: CVE-2024-22901

[[return to 192.168.186.129](#)]

2.1.9 High 80/tcp

High (CVSS: 7.5) NVT: Test HTTP dangerous methods
Summary ... continues on next page ...

<p>... continued from previous page ...</p> <p>Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.</p> <p>Quality of Detection (QoD): 99%</p> <p>Vulnerability Detection Result We could upload the following files via the PUT method at this web server: http://192.168.186.129/dav/puttest1596431571.html We could delete the following files via the DELETE method at this web server: http://192.168.186.129/dav/puttest1596431571.html</p> <p>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.</p> <p>Solution: Solution type: Mitigation Use access restrictions to these dangerous HTTP methods or disable them completely.</p> <p>Affected Software/OS Web servers with enabled PUT and/or DELETE methods.</p> <p>Vulnerability Detection Method 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</p> <p>References url: http://www.securityfocus.com/bid/12141 owasp: OWASP-CM-001</p>

<p>High (CVSS: 7.5)</p> <p>NVT: EasyPHP Webserver <= 12.1 Multiple Vulnerabilities - Active Check</p>
<p>Summary EasyPHP Webserver is prone to multiple vulnerabilities.</p>
<p>Quality of Detection (QoD): 99%</p>
<p>Vulnerability Detection Result ... continues on next page ...</p>

... continued from previous page ...
Vulnerable URL: <code>http://192.168.186.129/phpinfo.php</code> Concluded from: <pre><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 Core</h2> <h2>PHP Variables</h2></pre>
Impact Successful exploitation will allow attackers to gain administrative access, disclose the information, inject PHP code/shell and execute a remote PHP Code.
Solution: Solution type: 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.
Affected Software/OS EasyPHP version 12.1 and prior.
Vulnerability Insight The bug in EasyPHP WebServer Manager, its skipping authentication for certain requests. Which allows to bypass the authentication, disclose the information or execute a remote PHP code.
Vulnerability Detection Method Sends a crafted HTTP GET request and checks the response. Note: It is currently expected that a result of this VT is reported if the system is generally exposing a <code>phpinfo()</code> output on the relevant URL / endpoint (independent from the running product). Exposing such sensitive information is generally seen as a security misconfiguration and should be avoided. Details: <code>EasyPHP Webserver <= 12.1 Multiple Vulnerabilities - Active Check</code> OID:1.3.6.1.4.1.25623.1.0.803189 Version used: 2025-11-11T05:40:18Z
References url: https://cxsecurity.com/issue/WLB-2013040069

[[return to 192.168.186.129](#)]

2.1.10 High 2121/tcp

High (CVSS: 7.5)
NVT: FTP Brute Force Logins With Default Credentials Reporting
<p>Summary It was possible to login into the remote FTP server using weak/known credentials.</p>
<p>Quality of Detection (QoD): 95%</p>
<p>Vulnerability Detection Result It was possible to login with the following credentials <User>:<Password> msfadmin:msfadmin postgres:postgres service:service user:user </p>
<p>Impact This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.</p>
<p>Solution: Solution type: Mitigation Change the password as soon as possible.</p>
<p>Vulnerability Insight The following devices are / software is known to be affected:</p> <ul style="list-style-type: none"> - 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 - CVE-2018-25147: Microhard Systems IPn4G - CVE-2020-36915: Adtec Digital SignEdje Digital Signage Player <p>Note: As the VT 'FTP Brute Force Logins With Default Credentials' (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.</p>
<p>Vulnerability Detection Method Reports weak/known credentials detected by the VT 'FTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108717). Details: FTP Brute Force Logins With Default Credentials Reporting OID:1.3.6.1.4.1.25623.1.0.108718</p>
<p>... continues on next page ...</p>

<p>... continued from previous page ...</p> <p>Version used: 2026-01-16T15:42:49Z</p> <p>References</p> <p>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 cve: CVE-2018-25147 cve: CVE-2020-36915</p>

[[return to 192.168.186.129](#)]

2.1.11 High 6697/tcp

<p>High (CVSS: 8.1)</p> <p>NVT: UnrealIRCd Authentication Spoofing Vulnerability</p>
<p>Product detection result</p> <p>cpe:/a:unrealircd:unrealircd:3.2.8.1 Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)</p>
<p>Summary UnrealIRCd is prone to authentication spoofing vulnerability.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result Installed version: 3.2.8.1 Fixed version: 3.2.10.7</p>
<p>Impact Successful exploitation of this vulnerability will allow remote attackers to spoof certificate fingerprints and consequently log in as another user.</p>
<p>... continues on next page ...</p>

... continued from previous page ...
<p>Solution: Solution type: VendorFix Update to version 3.2.10.7, 4.0.6 or later.</p>
<p>Affected Software/OS UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.</p>
<p>Vulnerability Insight The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.</p>
<p>Vulnerability Detection Method 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: 2025-12-17T05:46:28Z</p>
<p>Product Detection Result Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection OID: 1.3.6.1.4.1.25623.1.0.809884)</p>
<p>References cve: CVE-2016-7144 url: http://seclists.org/oss-sec/2016/q3/420 url: http://www.securityfocus.com/bid/92763 url: http://www.openwall.com/lists/oss-security/2016/09/05/8 url: https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b ↳c50ba1a34a766 url: https://bugs.unrealircd.org/main_page.php</p>

High (CVSS: 7.5) NVT: UnrealIRCd Backdoor
<p>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)</p>
<p>Summary Detection of backdoor in UnrealIRCd.</p>
... continues on next page ...

	... continued from previous page ...
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.	
Affected Software/OS 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.	
Vulnerability Insight Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.	
Vulnerability Detection Method Details: UnrealIRCd Backdoor OID:1.3.6.1.4.1.25623.1.0.80111 Version used: 2025-03-21T05:38:29Z	
Product Detection Result Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection OID: 1.3.6.1.4.1.25623.1.0.809884)	
References cve: CVE-2010-2075 url: http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt url: http://seclists.org/fulldisclosure/2010/Jun/277 url: http://www.securityfocus.com/bid/40820	

[[return to 192.168.186.129](#)]

2.1.12 High 1099/tcp

High (CVSS: 7.5)
NVT: Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check
... continues on next page ...

	... continued from previous page ...
Summary	Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code (remote code execution/RCE) on a targeted system with elevated privileges.
Quality of Detection (QoD): 95%	
Vulnerability Detection Result	<p>By doing an RMI request it was possible to trigger the vulnerability and make the remote host sending a request back to the scanner host (Details on the received packet follows).</p> <p>Destination IP: 192.168.186.128 (receiving IP on scanner host side) Destination port: 31149/tcp (receiving port on scanner host side) Originating IP: 192.168.186.129 (originating IP from target host side)</p>
Impact	An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.
Solution:	
Solution type: Workaround	Disable class-loading. Please contact the vendor of the affected system for additional guidance.
Vulnerability Insight	The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software.
Vulnerability Detection Method	<p>Sends a crafted JRMI request and checks if the target is connecting back to the scanner host.</p> <p>Note: For a successful detection of this flaw the target host needs to be able to reach the scanner host on a TCP port randomly generated during the runtime of the VT (currently in the range of 10000-32000).</p> <p>Details: Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check OID:1.3.6.1.4.1.25623.1.0.140051 Version used: 2025-04-11T15:45:04Z</p>
References	<p>cve: CVE-2011-3556 url: https://web.archive.org/web/20211208040855/http://www.securitytracker.com/id?1026215 url: https://web.archive.org/web/20110824060234/http://download.oracle.com/java/1.3/docs/guide/rmi/spec/rmi-protocol.html url: https://tools.cisco.com/security/center/viewAlert.x?alertId=23665 dfn-cert: DFN-CERT-2012-1829 dfn-cert: DFN-CERT-2012-1380</p>
	... continues on next page ...

<pre>dfn-cert: DFN-CERT-2012-1377 dfn-cert: DFN-CERT-2012-1156 dfn-cert: DFN-CERT-2012-1155 dfn-cert: DFN-CERT-2012-0956 dfn-cert: DFN-CERT-2012-0828 dfn-cert: DFN-CERT-2012-0815 dfn-cert: DFN-CERT-2012-0638 dfn-cert: DFN-CERT-2012-0451 dfn-cert: DFN-CERT-2012-0418 dfn-cert: DFN-CERT-2012-0354 dfn-cert: DFN-CERT-2012-0146 dfn-cert: DFN-CERT-2012-0142 dfn-cert: DFN-CERT-2012-0126 dfn-cert: DFN-CERT-2012-0095 dfn-cert: DFN-CERT-2012-0047 dfn-cert: DFN-CERT-2011-1844 dfn-cert: DFN-CERT-2011-1826 dfn-cert: DFN-CERT-2011-1804 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</pre>	... continued from previous page ...
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------

<pre>dfn-cert: DFN-CERT-2012-1377 dfn-cert: DFN-CERT-2012-1156 dfn-cert: DFN-CERT-2012-1155 dfn-cert: DFN-CERT-2012-0956 dfn-cert: DFN-CERT-2012-0828 dfn-cert: DFN-CERT-2012-0815 dfn-cert: DFN-CERT-2012-0638 dfn-cert: DFN-CERT-2012-0451 dfn-cert: DFN-CERT-2012-0418 dfn-cert: DFN-CERT-2012-0354 dfn-cert: DFN-CERT-2012-0146 dfn-cert: DFN-CERT-2012-0142 dfn-cert: DFN-CERT-2012-0126 dfn-cert: DFN-CERT-2012-0095 dfn-cert: DFN-CERT-2012-0047 dfn-cert: DFN-CERT-2011-1844 dfn-cert: DFN-CERT-2011-1826 dfn-cert: DFN-CERT-2011-1804 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</pre>	... continued from previous page ...
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------

[[return to 192.168.186.129](#)]

2.1.13 High 5432/tcp

High (CVSS: 7.4)	
------------------	--

NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	
---------------------------------------------------------------------------	--

Summary	
----------------	--

OpenSSL is prone to a security bypass vulnerability.	
------------------------------------------------------	--

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

Vulnerability Detection Result	
---------------------------------------	--

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

Impact	
---------------	--

Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.	
------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

... continues on next page ...	
--------------------------------	--

	... continued from previous page ...
Solution: Solution type: VendorFix Updates are available. Please see the references for more information.	
Affected Software/OS OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.	
Vulnerability Insight OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.	
Vulnerability Detection Method Send two SSL ChangeCipherSpec request and check the response. 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: 2025-01-17T15:39:18Z	
References cve: CVE-2014-0224 url: https://www.openssl.org/news/secadv/20140605.txt url: http://www.securityfocus.com/bid/67899 cert-bund: WID-SEC-2026-0180 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	
... continues on next page ...	

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 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	... continued from previous page ...
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------

[[return to 192.168.186.129](#)]

2.1.14 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)
Summary

TWiki is prone to a cross-site request forgery (CSRF) vulnerability.

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

Installed version: 01.Feb.2003
Fixed version: 4.3.2

... continues on next page ...

<p>... continued from previous page ...</p> <p>Impact Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.</p> <p>Solution: Solution type: VendorFix Upgrade to TWiki version 4.3.2 or later.</p> <p>Affected Software/OS TWiki version prior to 4.3.2</p> <p>Vulnerability Insight 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.</p> <p>Vulnerability Detection Method 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</p> <p>References cve: CVE-2009-4898 url: http://www.openwall.com/lists/oss-security/2010/08/03/8 url: http://www.openwall.com/lists/oss-security/2010/08/02/17 url: http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix url: http://twiki.org/cgi-bin/view/Codev/DownloadTWiki</p>

<p>Medium (CVSS: 6.1)</p> <p>NVT: jQuery < 1.9.0 XSS Vulnerability</p>
<p>Summary jQuery is prone to a cross-site scripting (XSS) vulnerability.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result 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): - Identified file: http://192.168.186.129/mutillidae/javascript/ddsmoothmenu/jquery.min.js</p>

... continues on next page ...

<p>... continued from previous page ...</p> <p>- Referenced at: http://192.168.186.129/mutillidae/</p> <p>Solution: Solution type: VendorFix Update to version 1.9.0 or later.</p> <p>Affected Software/OS jQuery prior to version 1.9.0.</p> <p>Vulnerability Insight The jQuery(strInput) 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 '<' 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 '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.</p> <p>Vulnerability Detection Method 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</p> <p>References cve: CVE-2012-6708 url: https://bugs.jquery.com/ticket/11290 cert-bund: WID-SEC-2022-0673 cert-bund: CB-K22/0045 cert-bund: CB-K18/1131 dfn-cert: DFN-CERT-2025-1803 dfn-cert: DFN-CERT-2023-1197 dfn-cert: DFN-CERT-2020-0590</p>

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

	... continued from previous page ...
Fixed version:	6.1.0
Solution:	
Solution type:	VendorFix
Update to version 6.1.0 or later.	
Affected Software/OS	
TWiki version 6.0.2 and probably prior.	
Vulnerability Detection Method	
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	
References	
cve: CVE-2018-20212	
url: https://seclists.org/fulldisclosure/2019/Jan/7	
url: http://twiki.org/cgi-bin/view/Codev/DownloadTWiki	

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

... continued from previous page ...

Vulnerability Insight

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.

Vulnerability Detection Method

Details: TWiki CSRF Vulnerability

OID:1.3.6.1.4.1.25623.1.0.800400

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

References

cve: CVE-2009-1339

url: <http://secunia.com/advisories/34880>

url: <http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258>

url: <http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff-→-cve-2009-1339.txt>

Medium (CVSS: 5.8)

NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary

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.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

The web server has the following HTTP methods enabled: TRACE

Impact

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution:

Solution type: 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.

Affected Software/OS

Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight

... continues on next page ...

<p>... continued from previous page ...</p> <p>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.</p> <p>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</p> <p>References</p> <p>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 cert-bund: CB-K14/0981 dfn-cert: DFN-CERT-2021-1825 dfn-cert: DFN-CERT-2014-1018 dfn-cert: DFN-CERT-2010-0020</p>

Medium (CVSS: 5.3) NVT: phpinfo() Output Reporting (HTTP)
Summary Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The following files are calling the function phpinfo() which disclose potentially sensitive information: http://192.168.186.129/mutillidae/phpinfo.php Concluded from: <pre><title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head> <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/php5/cgi </td></tr> <h2>PHP Core</h2> <h2>PHP Variables</h2></pre> http://192.168.186.129/phpinfo.php Concluded from: <pre><title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head> <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/php5/cgi </td></tr> <h2>PHP Core</h2> <h2>PHP Variables</h2></pre>
Impact Some of the information that can be gathered from this file includes: 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.
Solution: Solution type: Workaround Delete the listed files or restrict access to them.
Affected Software/OS All systems exposing a file containing the output of the phpinfo() PHP function. This VT is also reporting if an affected endpoint for the following products have been identified: - CVE-2008-0149: TUTOS - CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK - CVE-2024-10486: Google for WooCommerce plugin for WordPress

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.

Vulnerability Detection Method

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: phpinfo() Output Reporting (HTTP)

OID:1.3.6.1.4.1.25623.1.0.11229

Version used: 2025-07-09T05:43:50Z

References

cve: CVE-2008-0149

cve: CVE-2023-49282

cve: CVE-2023-49283

cve: CVE-2024-10486

url: <https://www.php.net/manual/en/function.phpinfo.php>

url: <https://beaglesecurity.com/blog/vulnerability/revealing-phpinfo.html>

Medium (CVSS: 5.0)

NVT: /doc directory browsable

Summary

The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Vulnerable URL: http://192.168.186.129/doc/

Solution:

Solution type: Mitigation

Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:

```
<Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost
</Directory>
```

Vulnerability Detection Method

Details: /doc directory browsable

OID:1.3.6.1.4.1.25623.1.0.10056

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

... continues on next page ...

... continued from previous page ...

References

cve: CVE-1999-0678

url: <http://www.securityfocus.com/bid/318>

Medium (CVSS: 5.0)

NVT: awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check

Summary

awiki is prone to multiple local file include (LFI) vulnerabilities because it fails to properly sanitize user-supplied input.

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

Vulnerable URL: <http://192.168.186.129/mutillidae/index.php?page=/etc/passwd>

Impact

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.

Solution:

Solution type: 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.

Affected Software/OS

awiki version 20100125 and prior.

Vulnerability Detection Method

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: 2025-04-15T05:54:49Z

References

url: <https://www.exploit-db.com/exploits/36047/>

url: <http://www.securityfocus.com/bid/49187>

Medium (CVSS: 5.0)
NVT: QWikiwiki directory traversal vulnerability
Summary 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.
Quality of Detection (QoD): 99%
Vulnerability Detection Result Vulnerable URL: <code>http://192.168.186.129/mutillidae/index.php?page=../../../../etc/passwd%00</code>
Solution: Solution type: 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.
Vulnerability Detection Method Details: QWikiwiki directory traversal vulnerability OID:1.3.6.1.4.1.25623.1.0.16100 Version used: 2025-04-15T05:54:49Z
References cve: CVE-2005-0283 url: http://www.securityfocus.com/bid/12163

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP
Summary The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The following input fields were identified (URL:input name): <code>http://192.168.186.129/dvwa/login.php:password</code> <code>http://192.168.186.129/phpMyAdmin/:pma_password</code> <code>http://192.168.186.129/phpMyAdmin/?D=A:pma_password</code>
... continues on next page ...

<p style="text-align: right;">... continued from previous page ...</p> <pre>http://192.168.186.129/tikiwiki/tiki-install.php:pass http://192.168.186.129/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword</pre>
<p>Impact 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.</p>
<p>Solution: Solution type: 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.</p>
<p>Affected Software/OS Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.</p>
<p>Vulnerability Detection Method 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</p>
<p>References url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure url: https://cwe.mitre.org/data/definitions/319.html</p>

Medium (CVSS: 4.3) NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
<p>Summary phpMyAdmin is prone to a cross-site scripting (XSS) vulnerability.</p>
<p>Quality of Detection (QoD): 99%</p>
<p>Vulnerability Detection Result ... continues on next page ... </p>

... continued from previous page ...
Vulnerability was detected according to the Vulnerability Detection Method.
<p>Impact Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.</p>
<p>Solution: Solution type: 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.</p>
<p>Affected Software/OS phpMyAdmin version 3.3.8.1 and prior.</p>
<p>Vulnerability Insight 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.</p>
<p>Vulnerability Detection Method 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</p>
<p>References cve: CVE-2010-4480 url: http://www.exploit-db.com/exploits/15699/ url: http://www.vupen.com/english/advisories/2010/3133 dfn-cert: DFN-CERT-2011-0467 dfn-cert: DFN-CERT-2011-0451 dfn-cert: DFN-CERT-2011-0016 dfn-cert: DFN-CERT-2011-0002</p>

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
<p>Product detection result 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)</p>
<p>Summary ... continues on next page ...</p>

... continued from previous page ...
Apache HTTP Server is prone to a cookie information disclosure vulnerability.
Quality of Detection (QoD): 99%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
Solution: Solution type: VendorFix Update to Apache HTTP Server version 2.2.22 or later.
Affected Software/OS Apache HTTP Server versions 2.2.0 through 2.2.21.
Vulnerability Insight The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.
Vulnerability Detection Method Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.902830 Version used: 2025-03-05T05:38:53Z
Product Detection Result 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)
References cve: CVE-2012-0053 url: http://secunia.com/advisories/47779 url: http://www.securityfocus.com/bid/51706 url: http://www.exploit-db.com/exploits/18442 url: http://rhn.redhat.com/errata/RHSA-2012-0128.html url: http://httpd.apache.org/security/vulnerabilities_22.html url: http://svn.apache.org/viewvc?view=revision&revision=1235454 url: http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html cert-bund: CB-K15/0080 cert-bund: CB-K14/1505 cert-bund: CB-K14/0608 dfn-cert: DFN-CERT-2015-0082
... continues on next page ...

... continued from previous page ...

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
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

Medium (CVSS: 4.3)

NVT: jQuery < 1.6.3 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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: http://192.168.186.129/mutillidae/javascript/ddsmoothmenu/jquery.min.js
- Referenced at: http://192.168.186.129/mutillidae/

Solution:

Solution type: VendorFix

Update to version 1.6.3 or later.

Affected Software/OS

jQuery prior to version 1.6.3.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

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.

Vulnerability Detection Method

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

References

cve: CVE-2011-4969

url: <https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/>

cert-bund: CB-K17/0195

dfn-cert: DFN-CERT-2017-0199

dfn-cert: DFN-CERT-2016-0890

[[return to 192.168.186.129](#)]

2.1.15 Medium 2121/tcp

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

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

Impact

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:

Solution type: Mitigation

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method

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 192.168.186.129](#)]

2.1.16 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:1.3.6.1.4.1.25623.1.0.108528

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

References

url: <https://tools.ietf.org/html/rfc6143#page-10>

[[return to 192.168.186.129](#)]

2.1.17 Medium 22/tcp

Medium (CVSS: 5.3) NVT: Weak Host Key Algorithm(s) (SSH)
Product detection result cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 →)
Summary The remote SSH server is configured to allow / support weak host key algorithm(s).
Quality of Detection (QoD): 80%
Vulnerability Detection Result 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)
Solution: Solution type: Mitigation Disable the reported weak host key algorithm(s).
Vulnerability Detection Method 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
Product Detection Result Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)
References url: https://www.rfc-editor.org/rfc/rfc8332 url: https://www.rfc-editor.org/rfc/rfc8709 ... continues on next page ...

<p style="text-align: right;">... continued from previous page ...</p> <p>url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6</p>

<p>Medium (CVSS: 5.3)</p> <p>NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)</p>						
<p>Product detection result</p> <pre>cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 →)</pre>						
<p>Summary</p> <p>The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).</p>						
<p>Quality of Detection (QoD): 80%</p>						
<p>Vulnerability Detection Result</p> <p>The remote SSH server supports the following weak KEX algorithm(s):</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 60%;">KEX algorithm</th> <th style="text-align: left; width: 40%;">Reason</th> </tr> </thead> <tbody> <tr> <td>diffie-hellman-group-exchange-sha1</td> <td> Using SHA-1</td> </tr> <tr> <td>diffie-hellman-group1-sha1</td> <td> Using Oakley Group 2 (a 1024-bit MODP group →) and SHA-1</td> </tr> </tbody> </table>	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
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					
<p>Impact</p> <p>An attacker can quickly break individual connections.</p>						
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Disable the reported weak KEX algorithm(s)</p> <ul style="list-style-type: none"> - 1024-bit MODP group / prime KEX algorithms: <p>Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.</p>						
<p>Vulnerability Insight</p> <ul style="list-style-type: none"> - 1024-bit MODP group / prime KEX algorithms: <p>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.</p>						
<p>Vulnerability Detection Method</p> <p>Checks the supported KEX algorithms of the remote SSH server.</p>						

... continues on next page ...

... continued from previous page ...

Currently weak KEX algorithms are defined as the following:
 - non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
 - ephemeral 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
 OID: 1.3.6.1.4.1.25623.1.0.105565)

References

url: <https://weakdh.org/sysadmin.html>
 url: <https://www.rfc-editor.org/rfc/rfc9142>
 url: <https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implementations>
 url: <https://www.rfc-editor.org/rfc/rfc6194>
 url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.5>

Medium (CVSS: 4.3)

NVT: Weak Encryption Algorithm(s) Supported (SSH)

Product detection result

cpe:/a:ietf:secure_shell_protocol
 Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
 ↳)

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

The remote SSH server supports the following weak client-to-server encryption algorithms:
 ↳
 3des-cbc
 aes128-cbc
 aes192-cbc
 aes256-cbc
 arcfour
 arcfour128
 arcfour256

... continues on next page ...

<pre> 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 arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se </pre> <p>Solution: Solution type: Mitigation Disable the reported weak encryption algorithm(s).</p> <p>Vulnerability Insight</p> <ul style="list-style-type: none"> - 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. - 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. - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext. <p>Vulnerability Detection Method</p> <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"> - Arcfour (RC4) cipher based algorithms - 'none' algorithm - CBC mode cipher based algorithms <p>Details: Weak Encryption Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105611 Version used: 2024-06-14T05:05:48Z</p> <p>Product Detection Result</p> <p>Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)</p>	<p>... continued from previous page ...</p>

	... continued from previous page ...
--	--------------------------------------

References

url: <https://www.rfc-editor.org/rfc/rfc8758>
 url: <https://www.kb.cert.org/vuls/id/958563>
 url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.3>

[[return to 192.168.186.129](#)]

2.1.18 Medium 445/tcp

Medium (CVSS: 6.0)

NVT: Samba 3.0.0 <= 3.0.25rc3 MS-RPC Remote Shell Command Execution Vulnerability - Active Check

Product detection result

cpe:/a:samba:samba:3.0.20

Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary

Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.

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

By sending a special crafted SMB request it was possible to execute ‘‘ping -p 5f →4f70656e564153565438303230345f -c50 192.168.186.128’’ on the remote host.

Received answer (ICMP "Data" field):

0x00:	55 EB 8A 69 7A E7 04 00 56 54 38 30 32 30 34 5F	U..iz...VT80204_
0x10:	5F 4F 70 65 6E 56 41 53 56 54 38 30 32 30 34 5F	_OpenVASVT80204_
0x20:	5F 4F 70 65 6E 56 41 53 56 54 38 30 32 30 34 5F	_OpenVASVT80204_
0x30:	5F 4F 70 65 6E 56 41 53	_OpenVAS

Impact

An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.

Solution:

Solution type: VendorFix

Updates are available. Please see the referenced vendor advisory.

Affected Software/OS

Samba versions 3.0.0 through 3.0.25rc3.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method

Sends a crafted SMB request and checks if the target is connecting back to the scanner host.
Note: For a successful detection of this flaw the scanner host needs to be able to directly receive ICMP echo requests from the target.

Details: Samba 3.0.0 <= 3.0.25rc3 MS-RPC Remote Shell Command Execution Vulnerability - .
↔..

OID:1.3.6.1.4.1.25623.1.0.108011

Version used: 2025-03-18T05:38:50Z

Product Detection Result

Product: cpe:/a:samba:samba:3.0.20

Method: SMB_NativeLanMan

OID: 1.3.6.1.4.1.25623.1.0.102011)

References

cve: CVE-2007-2447

url: <https://www.samba.org/samba/security/CVE-2007-2447.html>

url: <https://web.archive.org/web/20210121173708/http://www.securityfocus.com/bid/23972>

[[return to 192.168.186.129](#)]

2.1.19 Medium 25/tcp

Medium (CVSS: 6.8)

NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability

Summary

Multiple vendors' implementations of 'STARTTLS' are prone to a vulnerability that lets attackers inject arbitrary commands.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

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.

... continues on next page ...

	... continued from previous page ...
Solution: Solution type: VendorFix Updates are available. Please see the references for more information.	
Affected Software/OS The following vendors are known to be affected: Ipswitch Kerio Postfix Qmail-TLS Oracle SCO Group spamdyke ISC	
Vulnerability Detection Method 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	
References cve: CVE-2011-0411 cve: CVE-2011-1430 cve: CVE-2011-1431 cve: CVE-2011-1432 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 url: 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 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 url: http://www.spamdyke.org/documentation/Changelog.txt url: http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include→_text=1 url: http://www.securityfocus.com/archive/1/516901	
... continues on next page ...	

... continued from previous page ...

```
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/cpupr2011-301950.html
url: http://inoa.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

Product detection result

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)

Summary

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and S \leftrightarrow SLv3 protocols and supports one or more ciphers. Those supported ciphers can b \leftrightarrow e found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256 \leftrightarrow 23.1.0.802067) VT.

... continues on next page ...

	... continued from previous page ...
Impact	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.
Solution:	Solution type: 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 resources supporting you with this task.
Affected Software/OS	All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
Vulnerability Insight	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)
Vulnerability Detection Method	Checks 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: 2025-03-27T05:38:50Z
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://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org
	... continues on next page ...

... continued from previous page ...

url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters->-report-2014>
url: <https://drownattack.com>
url: <https://www.imperialviolet.org/2014/10/14/poodle.html>
cert-bund: WID-SEC-2026-0180
cert-bund: WID-SEC-2025-1658
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
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

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

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

... continued from previous page ...

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 →ompliation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no su →ch thing outside US,C=XX (Server certificate)

Impact

Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Solution:

Solution type: Mitigation

Replace the certificate with a stronger key and reissue the certificates it signed.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

Vulnerability Detection Method
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

References
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25 ↔623.1.0.103692)

Summary
The remote server's SSL/TLS certificate has already expired.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
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,O=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

... continues on next page ...

<p style="text-align: right;">... continued from previous page ...</p> <pre>→30342D626173652E6C6F63616C646F6D61696E,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 subject alternative names (SAN) None valid from 2010-03-17 14:07:45 UTC valid until 2010-04-16 14:07:45 UTC</pre> <p>Solution:</p> <p>Solution type: Mitigation Replace the SSL/TLS certificate by a new one.</p> <p>Vulnerability Insight This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.</p> <p>Vulnerability Detection Method Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2024-06-14T05:05:48Z</p> <p>Product Detection Result 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)</p>

Medium (CVSS: 5.0) NVT: Check if Mailserver answer to VRFY and EXPN requests
<p>Summary The Mailserver on this host answers to VRFY and/or EXPN requests.</p>
<p>Quality of Detection (QoD): 99%</p>
<p>Vulnerability Detection Result 'VRFY root' produces the following answer: 252 2.0.0 root</p>
<p>Solution:</p> <p>Solution type: 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.</p>

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
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.

Vulnerability Detection Method
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

References
url: http://cr.yp.to/smtp/vrfy.html

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

Summary
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

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

Impact

The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:

Solution type: 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.

Affected Software/OS

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...
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.
Vulnerability Detection Method 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
References cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 cert-bund: WID-SEC-2026-0180 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0796 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K14/0772 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2025-0933 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: 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.)

... continues on next page ...

<p>→802067)</p>	<p>... continued from previous page ...</p>
	<p>Summary This host is accepting 'RSA_EXPORT' cipher suites and is prone to a man-in-the-middle (MITM) vulnerability.</p>
	<p>Quality of Detection (QoD): 80%</p>
	<p>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</p>
	<p>Impact 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.</p>
	<p>Solution: Solution type: VendorFix <ul style="list-style-type: none"> - Remove support for 'RSA_EXPORT' cipher suites from the service. Please see the references for more resources supporting you with this task. - If the service is using OpenSSL: Update to version 0.9.8zd, 1.0.0p, 1.0.1k or later. </p>
	<p>Affected Software/OS <ul style="list-style-type: none"> - Hosts accepting 'RSA_EXPORT' cipher suites. - OpenSSL versions prior to 0.9.8zd, 1.0.0 prior to 1.0.0p and 1.0.1 prior to 1.0.1k. </p>
	<p>Vulnerability Insight Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.</p>
	<p>Vulnerability Detection Method Checks previous collected cipher suites. 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: 2025-03-27T05:38:50Z</p>
	<p>... continues on next page ...</p>

... continued from previous page ...

Product Detection Result

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)

References

cve: CVE-2015-0204
url: <https://freakattack.com>
url: <https://openssl-library.org/news/secadv/20150108.txt>
url: <https://web.archive.org/web/20210122095002/http://www.securityfocus.com/bid/71936>
url: <https://www.secpod.com/blog/freak-attack>
url: <https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa>
url: <https://ssl-config.mozilla.org>
url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>
url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html
url: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html
url: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>
url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>
cert-bund: WID-SEC-2026-0180
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-K15/0016

... continues on next page ...

... continued from previous page ...

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: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result

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)

Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

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.

Impact

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.

... continues on next page ...

... continued from previous page ...

Solution:**Solution type:** 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 resources supporting you with this task.

Affected Software/OS

- All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols
- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder
- CVE-2024-41270: Gorush v1.18.4
- CVE-2025-3200: Multiple products from Wiesemann & Theis

Vulnerability Insight

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)

Vulnerability Detection Method

Checks 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: 2025-04-30T05:39:51Z

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-2011-3389

cve: CVE-2015-0204

cve: CVE-2023-41928

cve: CVE-2024-41270

cve: CVE-2025-3200

url: <https://ssl-config.mozilla.org>

url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>

url: https://www.bsi.bund.de/EN/Themen/Offentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html

url: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>

url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html

url: [https://www.bettercrypto.org](https://web.archive.org/web/20240113175943/https://www.bettercrypto.org)

... continues on next page ...

... continued from previous page ...

url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters->-report-2014>
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://certvde.com/en/advisories/VDE-2025-031/>
url: <https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc>
url: <https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273>
cert-bund: WID-SEC-2026-0180
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
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
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

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2012-0095

... continues on next page ...

... continued from previous page ...

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: 4.0)

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 Signature Algorithm: sha1WithRSAEncryption

Solution:

Solution type: 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.

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered crypto- graphically weak and not secure enough for ongoing use:

- | |
|-----------------------------------|
| - Secure Hash Algorithm 1 (SHA-1) |
|-----------------------------------|

... continues on next page ...

... continued from previous page ...

- 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

Vulnerability Detection Method

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

References

url: <https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with->sha-1-based-signature-algorithms/>

Medium (CVSS: 4.0)

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Server Temporary Key Size: 1024 bits

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:

Solution type: Workaround

- Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. Please see the references for more resources supporting you with this task.
- 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.

... continues on next page ...

<p>... continued from previous page ...</p> <p>Affected Software/OS All services providing an encrypted communication using Diffie-Hellman groups with insufficient strength.</p> <p>Vulnerability Insight 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.</p> <p>Vulnerability Detection Method Checks the DHE temporary public key size. Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabiliti. ↔.. OID:1.3.6.1.4.1.25623.1.0.106223 Version used: 2025-03-27T05:38:50Z</p> <p>References</p> <ul style="list-style-type: none"> url: https://weakdh.org url: https://weakdh.org/sysadmin.html url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 url: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile

[[return to 192.168.186.129](#)]

2.1.20 Medium 5432/tcp

Medium (CVSS: 5.9) NVT: SSL/TLS: Report Weak Cipher Suites
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. ... continues on next page ...

<p>→802067)</p>	<p>... continued from previous page ...</p>
	<p>Summary This routine reports all weak SSL/TLS cipher suites accepted by a service.</p>
	<p>Quality of Detection (QoD): 98%</p>
	<p>Vulnerability Detection Result '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</p>
	<p>Impact This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.</p>
	<p>Solution: Solution type: 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.</p>
	<p>Affected Software/OS All services providing an encrypted communication using weak SSL/TLS cipher suites.</p>
	<p>Vulnerability Insight These rules are applied for the evaluation of the cryptographic strength: <ul style="list-style-type: none"> - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong </p>
	<p>Vulnerability Detection Method Checks previous collected cipher suites. 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. Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: 2025-03-27T05:38:50Z</p>
	<p>Product Detection Result ... continues on next page ...</p>

... continued from previous page ...
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)
References cve: CVE-2013-2566 cve: CVE-2015-2808 cve: CVE-2015-4000 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 cert-bund: WID-SEC-2026-0180 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 ... continues on next page ...

... continued from previous page ...

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
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
cert-bund: CB-K13/0942
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

... continues on next page ...

<pre>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 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</pre>

... continued from previous page ...

<pre>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 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</pre>

<p>Medium (CVSS: 5.9)</p>

<p>NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection</p>

<h4>Product detection result</h4>

<p>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)</p>

<h4>Summary</h4>

<p>It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.</p>

<h4>Quality of Detection (QoD): 98%</h4>

<h4>Vulnerability Detection Result</h4>

<p>In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020) VT.</p>

<h4>Impact</h4>

<p>... continues on next page ...</p>

<p>... continued from previous page ...</p> <p>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.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p> <p>Solution: Solution type: 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 resources supporting you with this task.</p> <p>Affected Software/OS All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.</p> <p>Vulnerability Insight 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)</p> <p>Vulnerability Detection Method Checks 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: 2025-03-27T05:38:50Z</p> <p>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)</p> <p>References cve: CVE-2016-0800 cve: CVE-2014-3566 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</p>
<p>... continues on next page ...</p>

... continued from previous page ...

```
↔-report-2014
url: https://drownattack.com
url: https://www.imperialviolet.org/2014/10/14/poodle.html
cert-bund: WID-SEC-2026-0180
cert-bund: WID-SEC-2025-1658
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
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
```

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

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

... continued from previous page ...

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
 →ch thing outside US,C=XX (Server certificate)

Impact

Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Solution:

Solution type: Mitigation

Replace the certificate with a stronger key and reissue the certificates it signed.

... continues on next page ...

	... continued from previous page ...
Vulnerability Insight	SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.
Vulnerability Detection Method	<p>Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.</p> <p>Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048. ↳...</p> <p>OID:1.3.6.1.4.1.25623.1.0.150710</p> <p>Version used: 2021-12-10T12:48:00Z</p>
References	<p>url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf</p>

	Medium (CVSS: 5.0)																												
NVT: SSL/TLS: Certificate Expired																													
Product detection result	<p>cpe:/a:ietf:transport_layer_security</p> <p>Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25 ↳623.1.0.103692)</p>																												
Summary	The remote server's SSL/TLS certificate has already expired.																												
Quality of Detection (QoD): 99%																													
Vulnerability Detection Result	<p>The certificate of the remote service expired on 2010-04-16 14:07:45.</p> <p>Certificate details:</p> <table> <tbody> <tr> <td>fingerprint (SHA-1)</td> <td> ED093088706603BFD5DC237399B498DA2D4D31C6</td> </tr> <tr> <td>fingerprint (SHA-256)</td> <td> E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A</td> </tr> <tr> <td>→F1E32DEE436DE813CC</td> <td></td> </tr> <tr> <td>issued by</td> <td> 1.2.840.113549.1.9.1=#726F6F74407562756E747538</td> </tr> <tr> <td>→30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office</td> <td></td> </tr> <tr> <td>→ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is</td> <td></td> </tr> <tr> <td>→ no such thing outside US,C=XX</td> <td></td> </tr> <tr> <td>public key algorithm</td> <td> RSA</td> </tr> <tr> <td>public key size (bits)</td> <td> 1024</td> </tr> <tr> <td>serial</td> <td> 00FAF93A4C7FB6B9CC</td> </tr> <tr> <td>signature algorithm</td> <td> sha1WithRSAEncryption</td> </tr> <tr> <td>subject</td> <td> 1.2.840.113549.1.9.1=#726F6F74407562756E747538</td> </tr> <tr> <td>→30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office</td> <td></td> </tr> <tr> <td>→ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is</td> <td></td> </tr> </tbody> </table> <p>... continues on next page ...</p>	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,O=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,O=OCOSA,L=Everywhere,ST=There is	
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,O=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,O=OCOSA,L=Everywhere,ST=There is																													

<p>... continued from previous page ...</p> <pre>→ no such thing outside US,C=XX subject alternative names (SAN) None valid from 2010-03-17 14:07:45 UTC valid until 2010-04-16 14:07:45 UTC</pre> <p>Solution: Solution type: Mitigation Replace the SSL/TLS certificate by a new one.</p> <p>Vulnerability Insight This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.</p> <p>Vulnerability Detection Method Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2024-06-14T05:05:48Z</p> <p>Product Detection Result 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)</p>

<p>Medium (CVSS: 5.0)</p> <p>NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)</p> <p>Summary The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.</p> <p>Quality of Detection (QoD): 70%</p> <p>Vulnerability Detection Result 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</p> <hr/> <p>→ TLSv1.0 10</p> <p>Impact The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.</p> <p>Solution:</p>

... continues on next page ...

<p>... continued from previous page ...</p> <p>Solution type: 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.</p> <p>Affected Software/OS Every SSL/TLS service which does not properly restrict client-initiated renegotiation.</p> <p>Vulnerability Insight 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.</p> <p>Vulnerability Detection Method 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</p> <p>References</p> <p>cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 cert-bund: WID-SEC-2026-0180 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0796 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K14/0772 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2025-0933 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928</p>
<p>... continues on next page ...</p>

	... continued from previous page ...
	dfn-cert: DFN-CERT-2012-1112

Medium (CVSS: 4.3) NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Product detection result 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)
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection (QoD): 98%
Vulnerability Detection Result 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.
Impact 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.
Solution: Solution type: 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 resources supporting you with this task.
Affected Software/OS - All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols - CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder - CVE-2024-41270: Gorush v1.18.4 - CVE-2025-3200: Multiple products from Wiesemann & Theis
Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
... continues on next page ...

<p>... continued from previous page ...</p> <p>- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)</p> <p>Vulnerability Detection Method Checks 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: 2025-04-30T05:39:51Z</p> <p>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)</p> <p>References</p> <p>cve: CVE-2011-3389 cve: CVE-2015-0204 cve: CVE-2023-41928 cve: CVE-2024-41270 cve: CVE-2025-3200 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 url: https://datatracker.ietf.org/doc/rfc8996/ url: https://vhacker.blogspot.com/2011/09/beast.html url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak url: https://certvde.com/en/advisories/VDE-2025-031/ url: https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc url: https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273 cert-bund: WID-SEC-2026-0180 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</p> <p>... continues on next page ...</p>

... continued from previous page ...

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
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
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
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

... continues on next page ...

... continued from previous page ...

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
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
Summary The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
Quality of Detection (QoD): 80%
Vulnerability Detection Result Server Temporary Key Size: 1024 bits
Impact An attacker might be able to decrypt the SSL/TLS communication offline.
Solution: Solution type: Workaround <ul style="list-style-type: none"> - Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. Please see the references for more resources supporting you with this task. - 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.
Affected Software/OS All services providing an encrypted communication using Diffie-Hellman groups with insufficient strength.
Vulnerability Insight 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.
Vulnerability Detection Method 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: 2025-03-27T05:38:50Z
References <ul style="list-style-type: none"> url: https://weakdh.org url: https://weakdh.org/sysadmin.html url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/ <p>... continues on next page ...</p>

... continued from previous page ...
<pre>→TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch →eRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes →tstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters →-report-2014 url: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile</pre>

<p>Medium (CVSS: 4.0)</p> <p>NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm</p>
<p>Summary</p> <p>The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>The following certificates are part of the certificate chain but using insecure signature algorithms:</p> <p>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</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>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.</p>
<p>Vulnerability Insight</p> <p>The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:</p> <ul style="list-style-type: none"> - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) <p>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.</p>
<p>... continues on next page ...</p>

... continued from previous page ...

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

Vulnerability Detection Method

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

References

url: <https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with->sha-1-based-signature-algorithms/>

[[return to 192.168.186.129](#)]

2.1.21 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)

... continues on next page ...

... continued from previous page ...

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: 2025-01-21T05:37:33Z

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 192.168.186.129](#)]

2.1.22 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

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

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 144260

Packet 2: 144375

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'. Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: TCP Timestamps Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: 2023-12-15T16:10:08Z

References

url: <https://datatracker.ietf.org/doc/html/rfc1323>
 url: <https://datatracker.ietf.org/doc/html/rfc7323>
 url: <https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152>
 url: <https://www.fortiguard.com/psirt/FG-IR-16-090>

[[return to 192.168.186.129](#)]

2.1.23 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result

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 MAC algorithm(s).
Quality of Detection (QoD): 80%	
Vulnerability Detection Result	<p>The remote SSH server supports the following weak client-to-server MAC algorithm ↔(s):</p> <p>hmac-md5 hmac-md5-96 hmac-sha1-96 umac-64@openssh.com</p> <p>The remote SSH server supports the following weak server-to-client MAC algorithm ↔(s):</p> <p>hmac-md5 hmac-md5-96 hmac-sha1-96 umac-64@openssh.com</p>
Solution:	<p>Solution type: Mitigation</p> <p>Disable the reported weak MAC algorithm(s).</p>
Vulnerability Detection Method	<p>Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.</p> <p>Currently weak MAC algorithms are defined as the following:</p> <ul style="list-style-type: none">- MD5 based algorithms- 96-bit based algorithms- 64-bit based algorithms- 'none' algorithm <p>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</p>
Product Detection Result	<p>Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)</p>
References	<p>url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4</p>

2.1.24 Low 25/tcp

Low (CVSS: 3.7) NVT: SSL/TLS: 'DHE_EXPORT' MITM Security Bypass Vulnerability (LogJam)
<p>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)</p>
<p>Summary This host is accepting 'DHE_EXPORT' cipher suites and is prone to a man-in-the-middle (MITM) vulnerability.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result '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</p>
<p>Impact 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.</p>
<p>Solution: Solution type: VendorFix - Remove support for 'DHE_EXPORT' cipher suites from the service. Please see the references for more resources supporting you with this task. - If the service is using OpenSSL: Update to version 1.0.1n, 1.0.2b or later.</p>
<p>Affected Software/OS - Hosts accepting 'DHE_EXPORT' cipher suites. - OpenSSL versions prior to 1.0.1n and 1.0.2 prior to 1.0.2b.</p>
<p>Vulnerability Insight Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.</p>
... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method

Checks previous collected cipher suites.

Details: SSL/TLS: 'DHE_EXPORT' MITM Security Bypass Vulnerability (LogJam)

OID:1.3.6.1.4.1.25623.1.0.805188

Version used: 2025-03-27T05:38:50Z

Product Detection Result

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)

References

cve: CVE-2015-4000

url: <https://weakdh.org>

url: <https://weakdh.org/sysadmin.html>url: <https://web.archive.org/web/20210122160144/http://www.securityfocus.com/bid/74733>url: <https://weakdh.org/imperfect-forward-secrecy.pdf>url: <https://openwall.com/lists/oss-security/2015/05/20/8>url: <https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained>url: <https://openssl-library.org/post/2015-05-20-logjam-freak-upcoming-changes/index.html>url: <https://ssl-config.mozilla.org>url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.htmlurl: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.htmlurl: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>

cert-bund: WID-SEC-2026-0180

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

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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

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

Summary

This host is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Solution:

Solution type: Mitigation

Possible Mitigations are:

- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight

... continues on next page ...

... continued from previous page ...
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
Vulnerability Detection Method 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
Product Detection Result 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)
References cve: CVE-2014-3566 url: https://www.openssl.org/~bodo/ssl-poodle.pdf url: http://www.securityfocus.com/bid/70574 url: https://www.imperialviolet.org/2014/10/14/poodle.html url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin ↔g-ssl-30.html cert-bund: WID-SEC-2026-0180 cert-bund: WID-SEC-2025-1658 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
... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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 192.168.186.129](#)]

2.1.25 Low 5432/tcp

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 Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.→802067)
Summary This host is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
Solution: Solution type: Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
Vulnerability Insight The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method

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

Product Detection Result

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)

References

cve: CVE-2014-3566

url: <https://www.openssl.org/~bodo/ssl-poodle.pdf>

url: <http://www.securityfocus.com/bid/70574>

url: <https://www.imperialviolet.org/2014/10/14/poodle.html>url: <https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html>url: <http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin>
→g-ssl-30.html

cert-bund: WID-SEC-2026-0180

cert-bund: WID-SEC-2025-1658

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

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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 192.168.186.129](#)]

This file was automatically generated.