

Scan Report

May 23, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Metasploitable ”. The scan started at Fri May 23 20:30:37 2025 UTC and ended at Fri May 23 21:05:51 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1	Result Overview	2
1.1	Host Authentications	2
2	Results per Host	2
2.1	192.168.29.195	2
2.1.1	High 8009/tcp	4
2.1.2	High 514/tcp	10
2.1.3	High 3632/tcp	11
2.1.4	High 6200/tcp	12
2.1.5	High 5900/tcp	13
2.1.6	High general/tcp	14
2.1.7	High 21/tcp	15
2.1.8	High 80/tcp	17
2.1.9	High 8787/tcp	24
2.1.10	High 3306/tcp	25
2.1.11	High 1099/tcp	26
2.1.12	High 2121/tcp	28
2.1.13	High 513/tcp	30
2.1.14	High 512/tcp	31
2.1.15	High 5432/tcp	32
2.1.16	High 6697/tcp	35
2.1.17	High 1524/tcp	37

2.1.18	Medium 25/tcp	38
2.1.19	Medium 5900/tcp	57
2.1.20	Medium 21/tcp	57
2.1.21	Medium 80/tcp	59
2.1.22	Medium 23/tcp	73
2.1.23	Medium 2121/tcp	74
2.1.24	Medium 5432/tcp	74
2.1.25	Medium 445/tcp	92
2.1.26	Medium 22/tcp	93
2.1.27	Low 25/tcp	97
2.1.28	Low general/tcp	104
2.1.29	Low general/icmp	105
2.1.30	Low 5432/tcp	106
2.1.31	Low 22/tcp	109
2.1.32	Log 8009/tcp	110
2.1.33	Log 514/tcp	111
2.1.34	Log 25/tcp	111
2.1.35	Log 3632/tcp	128
2.1.36	Log 5900/tcp	128
2.1.37	Log general/tcp	130
2.1.38	Log 21/tcp	137
2.1.39	Log 80/tcp	139
2.1.40	Log 139/tcp	151
2.1.41	Log 8787/tcp	152
2.1.42	Log 3306/tcp	152
2.1.43	Log 23/tcp	154
2.1.44	Log 111/tcp	156
2.1.45	Log 1099/tcp	158
2.1.46	Log 2121/tcp	159
2.1.47	Log general/CPE-T	161
2.1.48	Log 53/tcp	162
2.1.49	Log 513/tcp	163
2.1.50	Log 512/tcp	163
2.1.51	Log 5432/tcp	165
2.1.52	Log 6697/tcp	175
2.1.53	Log 445/tcp	176
2.1.54	Log 1524/tcp	181
2.1.55	Log 22/tcp	182

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.29.195	24	40	6	90	0
Total: 1	24	40	6	90	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 “High” are not shown.

Issues with the threat level “Medium” are not shown.

Issues with the threat level “Low” are not shown.

Issues with the threat level “Log” are not shown.

Issues with the threat level “Debug” are not shown.

Issues with the threat level “False Positive” are not shown.

Only results with a minimum QoD of 70 are shown.

This report contains all 160 results selected by the filtering described above. Before filtering there were 621 results.

1.1 Host Authentications

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

2 Results per Host

2.1 192.168.29.195

Host scan start Fri May 23 20:31:41 2025 UTC

Host scan end Fri May 23 21:05:41 2025 UTC

Service (Port)	Threat Level
8009/tcp	High
514/tcp	High
3632/tcp	High
6200/tcp	High
5900/tcp	High
general/tcp	High
21/tcp	High

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
80/tcp	High
8787/tcp	High
3306/tcp	High
1099/tcp	High
2121/tcp	High
513/tcp	High
512/tcp	High
5432/tcp	High
6697/tcp	High
1524/tcp	High
25/tcp	Medium
5900/tcp	Medium
21/tcp	Medium
80/tcp	Medium
23/tcp	Medium
2121/tcp	Medium
5432/tcp	Medium
445/tcp	Medium
22/tcp	Medium
25/tcp	Low
general/tcp	Low
general/icmp	Low
5432/tcp	Low
22/tcp	Low
8009/tcp	Log
514/tcp	Log
25/tcp	Log
3632/tcp	Log
5900/tcp	Log
general/tcp	Log
21/tcp	Log
80/tcp	Log
139/tcp	Log
8787/tcp	Log
3306/tcp	Log
23/tcp	Log
111/tcp	Log
1099/tcp	Log
2121/tcp	Log
general/CPE-T	Log
53/tcp	Log
513/tcp	Log
512/tcp	Log
5432/tcp	Log

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
6697/tcp	Log
445/tcp	Log
1524/tcp	Log
22/tcp	Log

2.1.1 High 8009/tcp

High (CVSS: 9.8)

NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

Summary

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

Quality of Detection (QoD): 99%

Vulnerability Detection Result

It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.
Result:

```
AB 8\x0004 Ã\x0088 \x00020K \x0001 \x000CContent-Type \x001Ctext/html; charset=
↳ISO-8859-1 AB\x001FÃ¼\x0003\x001FÃ, <!--
```

```
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at
```

```
http://www.apache.org/licenses/LICENSE-2.0
```

```
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
```

```
-->
```

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
```

```
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
```

```
<head>
```

```
<title>Apache Tomcat/5.5</title>
```

```
<style type="text/css">
```

```
/*<![CDATA[*]
```

```
body {
```

... continues on next page ...

...continued from previous page ...

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

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

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

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

...continues on next page ...

...continued from previous page ...

```

        text-align: right;
        font-size: 80%;
    }
    /*]]>*/
</style>
</head>
<body>
<!-- Header -->
<table id="banner" width="100%">
    <tr>
        <td align="left" style="width:130px">
            <a href="http://tomcat.apache.org/">
                
            </a>
        </td>
        <td align="left" valign="top"><b>Apache Tomcat/5.5</b></td>
        <td align="right">
            <a href="http://www.apache.org/">
                
            </a>
        </td>
    </tr>
</table>
<table>
    <tr>
        <!-- Table of Contents -->
        <td valign="top">
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
<th>Administration</th>
                </tr>
                <tr>
<td class="menu">
                    <a href="manager/status">Status</a><br/>
                    <a href="admin">Tomcat&nbsp;Administration</a><br/>
                    <a href="manager/html">Tomcat&nbsp;Manager</a><br/>
                    &nbsp;
                </td>
                </tr>
            </table>
<br />
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
<th>Documentation</th>
                </tr>
            </table>
        </td>
    </tr>
</table>

```

...continues on next page ...

```

...continued from previous page ...

        <tr>
            <td class="menu">
                <a href="RELEASE-NOTES.txt">Release&nbsp;Notes</a><br/>
                <a href="tomcat-docs/changelog.html">Change&nbsp;Log</a><br/>
        ↪
                <a href="tomcat-docs">Tomcat&nbsp;Documentation</a><br/>
        ↪
                &nbsp;
                &nbsp;
            </td>
        </tr>
    </table>

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

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

```


... continued from previous page ...

```

    &nbsp;
    </td>
  </tr>
</table>

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

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

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

  <p>where "${CATALINA_HOME}" is the root of the Tomcat installation direc
  ↪tory. If you're seeing this page, and you don't think you should be, then eith
  ↪er you're either a user who has arrived at new installation of Tomcat, or you'
  ↪re an administrator who hasn't got his/her setup quite right. Providing the la
  ↪tter is the case, please refer to the <a href="tomcat-docs">Tomcat Documentati
  ↪on</a> for more detailed setup and administration information than is found in
  ↪ the INSTALL file.</p>

  <p><b>NOTE:</b> This page is precompiled. If you change it, this pag
  ↪e will not change since
    it was compiled into a servlet at build time.
    (See <tt>${CATALINA_HOME}/webapps/ROOT/WEB-INF/web.xml</tt> as t
  ↪o how it was mapped.)
  </p>
  <p><b>NOTE: For security reasons, using the administration webapp
  ... continues on next page ...

```

<p>...continued from previous page ...</p> <pre> is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in <code>\$CATALINA_HOME/conf/tomcat-users.xml</cod ↵e>.</p> <p>Included with this release are a host of sample Servlets and JSPs ↵ (with associated source code), extensive documentation (including the Servlet ↵ 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web app ↵lications.</p> <p>Tomcat mailing lists are available at the Tomcat project web site ↵:</p> users@tomc </pre>
<p>Solution: Solution type: VendorFix Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later. For other products using Tomcat please contact the vendor for more information on fixed versions.</p>
<p>Affected Software/OS Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled. Other products like JBoss or Wildfly which are using Tomcat might be affected as well.</p>
<p>Vulnerability Insight Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code.</p>
<p>Vulnerability Detection Method Sends a crafted AJP request and checks the response. Details: Apache Tomcat AJP RCE Vulnerability (Ghostcat) OID:1.3.6.1.4.1.25623.1.0.143545 Version used: 2025-01-21T05:37:33Z</p>
<p>References cve: CVE-2020-1938 cisa: Known Exploited Vulnerability (KEV) catalog url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog url: https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1↵a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E url: https://www.chaitin.cn/en/ghostcat url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487 url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances↵-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/ url: https://tomcat.apache.org/tomcat-7.0-doc/changelog.html url: https://tomcat.apache.org/tomcat-8.5-doc/changelog.html</p>
<p>... continues on next page ...</p>

...continued from previous page ...
url: https://tomcat.apache.org/tomcat-9.0-doc/changelog.html
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

[\[return to 192.168.29.195 \]](#)

2.1.2 High 514/tcp

High (CVSS: 7.5)
NVT: rsh Unencrypted Cleartext Login
Summary This remote host is running a rsh service.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The rsh service is misconfigured so it is allowing connections without a password or with default root:root credentials.
Solution: Solution type: Mitigation Disable the rsh service and use alternatives like SSH instead.
Vulnerability Insight
... continues on next page ...

...continued from previous page ...
<p>rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network.</p> <p>Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.</p>
<p>Vulnerability Detection Method Details: <code>rsh Unencrypted Cleartext Login</code> OID:1.3.6.1.4.1.25623.1.0.100080 Version used: 2021-10-20T09:03:29Z</p>
<p>References cve: CVE-1999-0651</p>

[\[return to 192.168.29.195 \]](#)

2.1.3 High 3632/tcp

<p>High (CVSS: 9.3)</p> <p>NVT: DistCC RCE Vulnerability (CVE-2004-2687)</p>
<p>Summary DistCC is prone to a remote code execution (RCE) vulnerability.</p>
<p>Quality of Detection (QoD): 99%</p>
<p>Vulnerability Detection Result It was possible to execute the "id" command. Result: uid=1(daemon) gid=1(daemon)</p>
<p>Impact 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: Solution type: VendorFix Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references.</p>
<p>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.</p>
<p>... continues on next page ...</p>

...continued from previous page ...

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>↪ archives.bugtraq/2005-03/0183.html

dfn-cert: DFN-CERT-2019-0381

[\[return to 192.168.29.195 \]](#)**2.1.4 High 6200/tcp**

High (CVSS: 9.8)

NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary

vsftpd is prone to a backdoor vulnerability.

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

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

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

Solution:**Solution type:** VendorFix

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

Affected Software/OS

The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.

Vulnerability Insight

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

... continues on next page ...

...continued from previous page...
Vulnerability Detection Method Details: vsftpd Compromised Source Packages Backdoor Vulnerability OID:1.3.6.1.4.1.25623.1.0.103185 Version used: 2023-12-07T05:05:41Z
References cve: CVE-2011-2523 url: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bid/48539/ url: https://security.appspot.com/vsftpd.html

[\[return to 192.168.29.195 \]](#)

2.1.5 High 5900/tcp

High (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. Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked. Note as well that passwords can be max. 8 characters long.
Vulnerability Detection Method Details: VNC Brute Force Login OID:1.3.6.1.4.1.25623.1.0.106056
... continues on next page ...

...continued from previous page ...

Version used: 2021-07-23T07:56:26Z

[\[return to 192.168.29.195 \]](#)**2.1.6 High general/tcp**

High (CVSS: 10.0)

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

Product detection result

cpe:/o:canonical:ubuntu_linux:8.04

Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↔.105937)**Summary**

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

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

The "Ubuntu" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:canonical:ubuntu_linux:8.04

Installed version,

build or SP: 8.04

EOL date: 2013-05-09

EOL info: <https://wiki.ubuntu.com/Releases>**Impact**

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

Solution:**Solution type:** Mitigation

Update the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Note / Important: Please create an override for this result if the target host is a:

- Windows system with Extended Security Updates (ESU)
- System with additional 3rd-party / non-vendor security updates like e.g. from 'TuxCare', 'Freexian Extended LTS' or similar

Vulnerability Detection Method

... continues on next page ...

...continued from previous page ...
<p>Checks if an EOL version of an OS is present on the target host. Details: Operating System (OS) End of Life (EOL) Detection OID: 1.3.6.1.4.1.25623.1.0.103674 Version used: 2025-05-21T05:40:19Z</p>
<p>Product Detection Result Product: cpe:/o:canonical:ubuntu_linux:8.04 Method: OS Detection Consolidation and Reporting OID: 1.3.6.1.4.1.25623.1.0.105937)</p>

[\[return to 192.168.29.195 \]](#)

2.1.7 High 21/tcp

<p>High (CVSS: 9.8)</p> <p>NVT: vsftpd Compromised Source Packages Backdoor Vulnerability</p>
<p>Product detection result cpe:/a:beasts:vsftpd:2.3.4 Detected by vsFTPd FTP Server Detection (OID: 1.3.6.1.4.1.25623.1.0.111050)</p>
<p>Summary vsftpd is prone to a backdoor vulnerability.</p>
<p>Quality of Detection (QoD): 99%</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.</p>
<p>Solution: Solution type: VendorFix The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.</p>
<p>Affected Software/OS The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.</p>
<p>Vulnerability Insight</p>
<p>... continues on next page ...</p>

...continued from previous page ...
The tainted source package contains a backdoor which opens a shell on port 6200/tcp.
Vulnerability Detection Method Details: vsftpd Compromised Source Packages Backdoor Vulnerability OID:1.3.6.1.4.1.25623.1.0.103185 Version used: 2023-12-07T05:05:41Z
Product Detection Result Product: cpe:/a:beasts:vsftpd:2.3.4 Method: vsFTPd FTP Server Detection OID: 1.3.6.1.4.1.25623.1.0.111050)
References cve: CVE-2011-2523 url: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bid/48539/ url: https://security.appspot.com/vsftpd.html

High (CVSS: 7.5)
NVT: FTP Brute Force Logins With Default Credentials Reporting
Summary It was possible to login into the remote FTP server using weak/known credentials.
Quality of Detection (QoD): 95%
Vulnerability Detection Result It was possible to login with the following credentials <User>:<Password> msfadmin:msfadmin postgres:postgres service:service user:user
Impact This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.
Solution: Solution type: Mitigation Change the password as soon as possible.
... continues on next page ...

...continued from previous page...

Vulnerability Insight

The following devices are / software is known to be affected:

- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2014-9198: Schneider Electric ETG3000 FactoryCast HMI gateways
- CVE-2015-7261: QNAP iArtist Lite distributed with QNAP Signage Station
- CVE-2016-8731: Foscam C1 devices
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-9068: IMM2 for IBM and Lenovo System x
- CVE-2018-17771: Ingenico Telium 2 PoS terminals
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices

Note: As the VT 'FTP Brute Force Logins 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.

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

Version used: 2025-05-13T05:41:39Z

References

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

[\[return to 192.168.29.195 \]](#)

2.1.8 High 80/tcp

High (CVSS: 10.0) NVT: TWiki XSS and Command Execution Vulnerabilities
Summary TWiki is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 4.2.4
Impact Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.
Solution: Solution type: VendorFix Upgrade to version 4.2.4 or later.
Affected Software/OS TWiki, TWiki version prior to 4.2.4.
Vulnerability Insight The flaws are due to: - %URLPARAM}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack. - %SEARCH}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.
Vulnerability Detection Method Details: TWiki XSS and Command Execution Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.800320 Version used: 2024-03-01T14:37:10Z
References cve: CVE-2008-5304 cve: CVE-2008-5305 url: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304 url: http://www.securityfocus.com/bid/32668 url: http://www.securityfocus.com/bid/32669 url: http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305

<p>High (CVSS: 9.8)</p> <p>NVT: PHP < 5.6.30, 7.x < 7.0.15, 7.1.x < 7.1.1 Multiple Vulnerabilities (Jan 2017) - Linux</p>
<p>Product detection result</p> <p>cpe:/a:php:php:5.2.4</p> <p>Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary</p> <p>PHP is prone to multiple vulnerabilities.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.2.4</p> <p>Fixed version: 5.6.30</p> <p>Installation</p> <p>path / port: 80/tcp</p>
<p>Solution:</p> <p>Solution type: VendorFix</p> <p>Update to version 5.6.30, 7.0.15, 7.1.1 or later.</p>
<p>Affected Software/OS</p> <p>PHP prior to version 5.6.30, 7.x prior to 7.0.15 and 7.1.x prior to 7.1.1.</p>
<p>Vulnerability Insight</p> <p>The following flaws exist:</p> <ul style="list-style-type: none"> - CVE-2016-10161: Heap out of bounds read on unserialize in finish_nested_data() - CVE-2016-10158: FPE when parsing a tag format - CVE-2016-10168: Signed Integer Overflow gd_io.c - CVE-2016-10167: DOS vulnerability in gdImageCreateFromGd2Ctx() - CVE-2017-11147: Seg fault when loading hostile phar - CVE-2016-10160: Memory corruption when loading hostile phar - CVE-2016-10159: Crash while loading hostile phar archive
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: PHP < 5.6.30, 7.x < 7.0.15, 7.1.x < 7.1.1 Multiple Vulnerabilities (Jan 2017) - . ↪..</p> <p>OID:1.3.6.1.4.1.25623.1.0.108052</p> <p>Version used: 2025-05-21T05:40:19Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:php:php:5.2.4</p>
<p>... continues on next page ...</p>

...continued from previous page ...	
Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References cve: CVE-2017-11147 cve: CVE-2016-10158 cve: CVE-2016-10159 cve: CVE-2016-10160 cve: CVE-2016-10161 cve: CVE-2016-10167 cve: CVE-2016-10168 url: http://www.php.net/ChangeLog-5.php url: http://www.php.net/ChangeLog-7.php url: http://bugs.php.net/73825 url: http://bugs.php.net/73737 url: http://bugs.php.net/73869 url: http://bugs.php.net/73868 url: http://bugs.php.net/73773 url: http://bugs.php.net/73768 url: http://bugs.php.net/73764 cert-bund: WID-SEC-2023-2718 cert-bund: CB-K17/1957 cert-bund: CB-K17/1575 cert-bund: CB-K17/1461 cert-bund: CB-K17/1358 cert-bund: CB-K17/1252 cert-bund: CB-K17/0527 cert-bund: CB-K17/0327 cert-bund: CB-K17/0318 cert-bund: CB-K17/0269 cert-bund: CB-K17/0264 cert-bund: CB-K17/0232 cert-bund: CB-K17/0182 cert-bund: CB-K17/0141 dfn-cert: DFN-CERT-2018-0835 dfn-cert: DFN-CERT-2017-2044 dfn-cert: DFN-CERT-2017-1647 dfn-cert: DFN-CERT-2017-1529 dfn-cert: DFN-CERT-2017-1420 dfn-cert: DFN-CERT-2017-1295 dfn-cert: DFN-CERT-2017-0532 dfn-cert: DFN-CERT-2017-0334 dfn-cert: DFN-CERT-2017-0325 dfn-cert: DFN-CERT-2017-0274 dfn-cert: DFN-CERT-2017-0270 dfn-cert: DFN-CERT-2017-0234	
...continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2017-0179
 dfn-cert: DFN-CERT-2017-0144

High (CVSS: 9.8)

NVT: PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check

Summary

PHP is prone to multiple vulnerabilities.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

By doing the following HTTP POST request:

"HTTP POST" body : <?php phpinfo();?>

URL : http://192.168.29.195/cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%7
 ↪5%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D
 ↪%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%
 ↪6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+
 ↪%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%
 ↪72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%6
 ↪3%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E
 ↪%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E

it was possible to execute the "<?php phpinfo();?>" command.

Result:

```
<title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/cgi </td></tr>
<h2>PHP Variables</h2>
```

Impact

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

Solution:

Solution type: VendorFix

PHP: Update to version 5.3.13, 5.4.3 or later

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

Affected Software/OS

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

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

... continues on next page ...

...continued from previous page ...

Vulnerability Insight

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

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

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

Vulnerability Detection Method

Send multiple a crafted HTTP POST requests and checks the responses.

Note: This script checks for the presence of CVE-2012-1823 which indicates that the system is also affected by the other included CVEs.

Details: PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check

OID:1.3.6.1.4.1.25623.1.0.103482

Version used: 2025-04-24T05:40:00Z

References

cve: CVE-2012-1823

cve: CVE-2012-2311

cve: CVE-2012-2336

cve: CVE-2012-2335

url: <https://web.archive.org/web/20190212080415/http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/>

url: <https://www.kb.cert.org/vuls/id/520827>

url: <https://bugs.php.net/bug.php?id=61910>

url: <https://www.php.net/manual/en/security.cgi-bin.php>

url: <https://web.archive.org/web/20210121223743/http://www.securityfocus.com/bid/53388>

url: <https://web.archive.org/web/20120709064615/http://www.h-online.com/open/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

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0913
dfn-cert: DFN-CERT-2012-0907
dfn-cert: DFN-CERT-2012-0906
dfn-cert: DFN-CERT-2012-0900
dfn-cert: DFN-CERT-2012-0880
dfn-cert: DFN-CERT-2012-0878
```

High (CVSS: 7.5)**NVT: Test HTTP dangerous methods****Summary**

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

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

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

<http://192.168.29.195/dav/puttest383920464.html>

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

<http://192.168.29.195/dav/puttest383920464.html>

Impact

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

Solution:

Solution type: Mitigation

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

Affected Software/OS

Web servers with enabled PUT and/or DELETE methods.

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

References

url: <http://www.securityfocus.com/bid/12141>

... continues on next page ...

...continued from previous page ...
owasp: OWASP-CM-001

[\[return to 192.168.29.195 \]](#)

2.1.9 High 8787/tcp

High (CVSS: 10.0)
NVT: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities
<p>Summary</p> <p>Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.</p>
<p>Quality of Detection (QoD): 99%</p>
<p>Vulnerability Detection Result</p> <p>The service is running in \$SAFE >= 1 mode. However it is still possible to run a ↵rbbitrary syscall commands on the remote host. Sending an invalid syscall the s ↵ervice returned the following response:</p> <pre>Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'syscall'"0/usr/lib/ ↵ruby/1.8/drb/drb.rb:1555:in 'send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in '__se ↵nd__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'perform_without_block'"3/usr/lib/ ↵ruby/1.8/drb/drb.rb:1515:in 'perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in 'm ↵ain_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in 'loop'"5/usr/lib/ruby/1.8/drb/ ↵drb.rb:1585:in 'main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in 'start'"5/usr ↵/lib/ruby/1.8/drb/drb.rb:1581:in 'main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:143 ↵0:in 'run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in 'start'"//usr/lib/ruby/1.8/dr ↵b/drb.rb:1427:in 'run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in 'initialize'"//us ↵r/lib/ruby/1.8/drb/drb.rb:1627:in 'new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in ↵'start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im ↵plemented</pre>
<p>Impact</p> <p>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.</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:</p> <ul style="list-style-type: none"> - Implementing taint on untrusted input
... continues on next page ...

...continued from previous page ...
<div>- Setting \$SAFE levels appropriately (≥ 2 is recommended if untrusted hosts are allowed to submit Ruby commands, and ≥ 3 may be appropriate)</div> <div>- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts</div>
<div>Vulnerability Detection Method</div> <div>Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.</div> <div>Details: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities</div> <div>OID:1.3.6.1.4.1.25623.1.0.108010</div> <div>Version used: 2024-06-28T05:05:33Z</div>
<div>References</div> <div>url: https://tools.cisco.com/security/center/viewAlert.x?alertId=22750</div> <div>url: http://www.securityfocus.com/bid/47071</div> <div>url: http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testing/</div> <div>url: http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html</div>

[\[return to 192.168.29.195 \]](#)

2.1.10 High 3306/tcp

<div>High (CVSS: 9.8)</div> <div>NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)</div>
<div>Product detection result</div> <div>cpe:/a:mysql:mysql:5.0.51a</div> <div>Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.25623.1.0.100152)</div>
<div>Summary</div> <div>It was possible to login into the remote MySQL using default credentials.</div>
<div>Quality of Detection (QoD): 95%</div>
<div>Vulnerability Detection Result</div> <div>It was possible to login as user "root" with an empty password.</div>
<div>Solution:</div> <div>Solution type: Mitigation</div> <div>- Change the password as soon as possible</div> <div>- Contact the vendor for other possible fixes / updates</div>
... continues on next page ...

...continued from previous page ...

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
 - CVE-2007-2554: Associated Press (AP) Newspaper 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: 2025-03-14T05:38:04Z

Product Detection Result

Product: cpe:/a:mysql:mysql:5.0.51a

Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

- cve: CVE-2015-4669
- 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-2016-6531
- cve: CVE-2018-15719
- cve: CVE-2024-22901

[\[return to 192.168.29.195 \]](#)

2.1.11 High 1099/tcp

High (CVSS: 7.5)	
NVT: Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check	
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 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). Destination IP: 192.168.29.114 (receiving IP on scanner host side) Destination port: 25759/tcp (receiving port on scanner host side) Originating IP: 192.168.29.195 (originating IP from target host side)	
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 Sends a crafted JRMI request and checks if the target is connecting back to the scanner host. 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). 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	
References 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/javas ... continues on next page ...	

Check

...continued from previous page ...

```

↪e/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
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

```

[\[return to 192.168.29.195 \]](#)**2.1.12 High 2121/tcp****High (CVSS: 7.5)****NVT: FTP Brute Force Logins With Default Credentials Reporting****Summary**

It was possible to login into the remote FTP server using weak/known credentials.

Quality of Detection (QoD): 95%**Vulnerability Detection Result**It was possible to login with the following credentials <User>:<Password>
msfadmin:msfadmin

...continues on next page ...

...continued from previous page ...	
postgres:postgres service:service user:user	
Impact This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.	
Solution: Solution type: Mitigation Change the password as soon as possible.	
Vulnerability Insight The following devices are / software is known to be affected: <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 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.	
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 Version used: 2025-05-13T05:41:39Z	
References 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	
...continues on next page ...	

...continued from previous page ...
cve: CVE-2018-17771
cve: CVE-2018-19063
cve: CVE-2018-19064

[\[return to 192.168.29.195 \]](#)

2.1.13 High 513/tcp

High (CVSS: 10.0)
NVT: rlogin Passwordless Login
Summary The rlogin service allows root access without a password.
Quality of Detection (QoD): 80%
Vulnerability Detection Result It was possible to gain root access without a password.
Impact This vulnerability allows an attacker to gain complete control over the target system.
Solution: Solution type: Mitigation Disable the rlogin service and use alternatives like SSH instead.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: rlogin Passwordless Login OID:1.3.6.1.4.1.25623.1.0.113766 Version used: 2020-09-30T09:30:12Z

High (CVSS: 7.5)
NVT: The rlogin service is running
Summary This remote host is running a rlogin service.
Quality of Detection (QoD): 80%
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result The rlogin service is running on the target system.
Solution: Solution type: Mitigation Disable the rlogin service and use alternatives like SSH instead.
Vulnerability Insight rlogin has several serious security problems, - all information, including passwords, is transmitted unencrypted. - .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password)
Vulnerability Detection Method Details: The rlogin service is running OID:1.3.6.1.4.1.25623.1.0.901202 Version used: 2025-03-05T05:38:53Z
References cve: CVE-1999-0651

[[return to 192.168.29.195](#)]

2.1.14 High 512/tcp

High (CVSS: 10.0) NVT: The rexec service is running
Summary This remote host is running a rexec service.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The rexec service was detected on the target system.
Solution: Solution type: Mitigation Disable the rexec service and use alternatives like SSH instead.
Vulnerability Insight rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer. ... continues on next page ...

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

[\[return to 192.168.29.195 \]](#)

2.1.15 High 5432/tcp

High (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.
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
Product Detection Result ... continues on next page ...

...continued from previous page ...

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

High (CVSS: 7.4)

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

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.

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-2023-0500

cert-bund: CB-K15/0567

... continues on next page ...

...continued from previous page...

cert-bund: CB-K15/0415
cert-bund: CB-K15/0384
cert-bund: CB-K15/0080
cert-bund: CB-K15/0079
cert-bund: CB-K15/0074
cert-bund: CB-K14/1617
cert-bund: CB-K14/1537
cert-bund: CB-K14/1299
cert-bund: CB-K14/1297
cert-bund: CB-K14/1294
cert-bund: CB-K14/1202
cert-bund: CB-K14/1174
cert-bund: CB-K14/1153
cert-bund: CB-K14/0876
cert-bund: CB-K14/0756
cert-bund: CB-K14/0746
cert-bund: CB-K14/0736
cert-bund: CB-K14/0722
cert-bund: CB-K14/0716
cert-bund: CB-K14/0708
cert-bund: CB-K14/0684
cert-bund: CB-K14/0683
cert-bund: CB-K14/0680
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0078
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1364
dfn-cert: DFN-CERT-2014-1357
dfn-cert: DFN-CERT-2014-1350
dfn-cert: DFN-CERT-2014-1265
dfn-cert: DFN-CERT-2014-1209
dfn-cert: DFN-CERT-2014-0917
dfn-cert: DFN-CERT-2014-0789
dfn-cert: DFN-CERT-2014-0778
dfn-cert: DFN-CERT-2014-0768
dfn-cert: DFN-CERT-2014-0752
dfn-cert: DFN-CERT-2014-0747
dfn-cert: DFN-CERT-2014-0738
dfn-cert: DFN-CERT-2014-0715
dfn-cert: DFN-CERT-2014-0714
dfn-cert: DFN-CERT-2014-0709

[\[return to 192.168.29.195 \]](#)

2.1.16 High 6697/tcp

High (CVSS: 8.1)
NVT: UnrealIRCd Authentication Spoofing Vulnerability
Product detection result cpe:/a:unrealircd:unrealircd:3.2.8.1 Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)
Summary UnrealIRCd is prone to authentication spoofing vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 3.2.8.1 Fixed version: 3.2.10.7
Impact Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.
Solution: Solution type: VendorFix Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.
Affected Software/OS UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.
Vulnerability Insight The flaw exists due to an error in the 'm__authenticate' function in 'modules/m__sasl.c' script.
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: 2023-07-14T16:09:27Z
Product Detection Result Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.809884)
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

High (CVSS: 7.5) NVT: UnrealIRCd Backdoor
Product detection result cpe: /a:unrealircd:unrealircd:3.2.8.1 Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)
Summary Detection of backdoor in UnrealIRCd.
Quality of Detection (QoD): 70%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution: Solution type: VendorFix Install latest version of unrealircd and check signatures of software you're installing.
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
... continues on next page ...

...continued from previous page...
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 192.168.29.195](#)]

2.1.17 High 1524/tcp

High (CVSS: 10.0) NVT: Possible Backdoor: Ingreslock
Summary A backdoor is installed on the remote host.
Quality of Detection (QoD): 99%
Vulnerability Detection Result The service is answering to an 'id;' command with the following response: uid=0(↪root) gid=0(root)
Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.
Solution: Solution type: Workaround A whole cleanup of the infected system is recommended.
Vulnerability Detection Method Details: Possible Backdoor: Ingreslock OID:1.3.6.1.4.1.25623.1.0.103549 Version used: 2023-07-25T05:05:58Z

[\[return to 192.168.29.195 \]](#)

2.1.18 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.
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 ... continues on next page ...

...continued from previous page...

```

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
url: http://support.avaya.com/css/P8/documents/100134676
url: http://support.avaya.com/css/P8/documents/100141041
url: http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html
url: http://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↵SSLv3 protocols and supports one or more ciphers. Those supported ciphers can b↵e found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256↵23.1.0.802067) VT.
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
... continues on next page ...

...continued from previous page ...
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/TechGuidel ↪ines/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/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://drownattack.com url: https://www.imperialviolet.org/2014/10/14/poodle.html 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
...continues on next page ...

...continued from previous page ...

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

...continues on next page ...

...continued from previous page ...

```

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

```

Medium (CVSS: 5.3)

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

Summary

... continues on next page ...

...continued from previous page ...	
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=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX (Server certificate)	
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.	
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: 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 ...continues on next page ...	

...continued from previous page...	
<p>The following indicates that the remote SSL/TLS service is affected:</p> <pre>Protocol Version Successful re-done SSL/TLS handshakes (Renegotiation) over an ↔ existing / already established SSL/TLS connection ----- ↔----- TLSv1.0 10</pre>	
<p>Impact</p> <p>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> <p>Solution type: VendorFix</p> <p>Users should contact their vendors for specific patch information.</p> <p>A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.</p>	
<p>Affected Software/OS</p> <p>Every SSL/TLS service which does not properly restrict client-initiated renegotiation.</p>	
<p>Vulnerability Insight</p> <p>The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.</p> <p>Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:</p> <p>> 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.</p> <p>Both CVEs are still kept in this VT as a reference to the origin of this flaw.</p>	
<p>Vulnerability Detection Method</p> <p>Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.</p> <p>Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)</p> <p>OID:1.3.6.1.4.1.25623.1.0.117761</p> <p>Version used: 2024-09-27T05:05:23Z</p>	
<p>References</p> <p>cve: CVE-2011-1473</p> <p>cve: CVE-2011-5094</p> <p>url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</p> <p>url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</p> <p>url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</p> <p>url: https://www.openwall.com/lists/oss-security/2011/07/08/2</p> <p>cert-bund: WID-SEC-2024-1591</p> <p>cert-bund: WID-SEC-2024-0796</p>	
... continues on next page ...	

...continued from previous page ...

```

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: 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

↪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

... continues on next page ...

...continued from previous page ...	
subject alternative names (SAN)	None
valid from	2010-03-17 14:07:45 UTC
valid until	2010-04-16 14:07:45 UTC
Solution: Solution type: Mitigation Replace the SSL/TLS certificate by a new one.	
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.	
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	
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)	

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

...continued from previous page ...
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: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↪802067)
Summary This host is accepting 'RSA_EXPORT' cipher suites and is prone to a man-in-the-middle (MITM) vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result 'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5
Impact 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.
Solution:
... continues on next page ...

...continued from previous page ...
Solution type: VendorFix - 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.
Affected Software/OS - 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.
Vulnerability Insight Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.
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
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/Mindeststandard_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
... continues on next page ...

...continued from previous page ...

```

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
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)

... continues on next page ...

...continued from previous page ...
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) - 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
... continues on next page ...

...continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105782)

References

cve: CVE-2011-3389

cve: CVE-2015-0204

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/TechGuidel↵ines/TG02102/BSI-TR-02102-1.html>url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/↵TLS-Protokoll/TLS-Protokoll_node.htmlurl: <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.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>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-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

... continues on next page ...

...continued from previous page ...

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
 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

...continues on next page ...

...continued from previous page ...

```

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

... continues on next page ...

...continued from previous page...	
Impact	An attacker might be able to decrypt the SSL/TLS communication offline.
Solution:	<p>Solution type: Workaround</p> <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	<p>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>
Vulnerability Detection Method	<p>Checks the DHE temporary public key size.</p> <p>Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability.</p> <p>↪..</p> <p>OID:1.3.6.1.4.1.25623.1.0.106223</p> <p>Version used: 2025-03-27T05:38:50Z</p>
References	<p>url: https://weakdh.org</p> <p>url: https://weakdh.org/sysadmin.html</p> <p>url: https://ssl-config.mozilla.org</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html</p> <p>url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/0TLS-Protokoll/TLS-Protokoll_node.html</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html</p> <p>url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org</p> <p>url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</p> <p>↪-report-2014</p> <p>url: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile</p>

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
<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</p> <p>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>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:</p> <p>Fingerprint1 or fingerprint1, Fingerprint2</p>
<p>Vulnerability Detection Method</p> <p>Check which hashing algorithm was used to sign the remote SSL/TLS certificate.</p> <p>Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm</p> <p>OID:1.3.6.1.4.1.25623.1.0.105880</p>
... continues on next page ...

...continued from previous page ...
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/

[\[return to 192.168.29.195 \]](#)

2.1.19 Medium 5900/tcp

Medium (CVSS: 4.8)
NVT: VNC Server Unencrypted Data Transmission
Summary The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.
Quality of Detection (QoD): 70%
Vulnerability Detection Result The VNC server provides the following insecure or cryptographically weak Security Type(s): 2 (VNC authentication)
Impact An attacker can uncover sensitive data by sniffing traffic to the VNC server.
Solution: Solution type: Mitigation Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.
Vulnerability Detection Method Details: VNC Server Unencrypted Data Transmission OID:1.3.6.1.4.1.25623.1.0.108529 Version used: 2023-07-12T05:05:04Z
References url: https://tools.ietf.org/html/rfc6143#page-10

[\[return to 192.168.29.195 \]](#)

2.1.20 Medium 21/tcp

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

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 Please specify the password. Anonymous sessions: 331 Please specify the password.
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.
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

[\[return to 192.168.29.195 \]](#)

2.1.21 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%
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 4.3.2
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 TWiki version 4.3.2 or later.
Affected Software/OS TWiki version prior to 4.3.2
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.
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
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
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: 6.1)	
NVT: jQuery < 1.9.0 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: 1.9.0 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://192.168.29.195/mutillidae/javascript/ddsmoothmenu/jquery.min.js - Referenced at: http://192.168.29.195/mutillidae/	
Solution: Solution type: VendorFix Update to version 1.9.0 or later.	
Affected Software/OS ... continues on next page ...	

...continued from previous page ...
jQuery prior to version 1.9.0.
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.
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
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-2023-1197 dfn-cert: DFN-CERT-2020-0590

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.
... continues on next page ...

...continued from previous page ...
Affected Software/OS TWiki version prior to 4.3.1
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 ... continues on next page ...

...continued from previous page...

Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight

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

Vulnerability Detection Method

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

Details: HTTP Debugging Methods (TRACE/TRACK) Enabled

OID:1.3.6.1.4.1.25623.1.0.11213

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

References

cve: CVE-2003-1567

cve: CVE-2004-2320

cve: CVE-2004-2763

cve: CVE-2005-3398

cve: CVE-2006-4683

cve: CVE-2007-3008

cve: CVE-2008-7253

cve: CVE-2009-2823

cve: CVE-2010-0386

cve: CVE-2012-2223

cve: CVE-2014-7883

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

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

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

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

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

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

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

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

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

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

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

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

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

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

url: https://owasp.org/www-community/attacks/Cross_Site_Tracing

cert-bund: CB-K14/0981

dfn-cert: DFN-CERT-2021-1825

dfn-cert: DFN-CERT-2014-1018

dfn-cert: DFN-CERT-2010-0020

Medium (CVSS: 5.3)
NVT: phpinfo() Output Reporting (HTTP)
<div><div>Summary</div><div>Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.</div></div>
<div>Quality of Detection (QoD): 80%</div>
<div><div>Vulnerability Detection Result</div><div>The following files are calling the function phpinfo() which disclose potentiall ↵y sensitive information: http://192.168.29.195/mutillidae/phpinfo.php Concluded from: <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV ↵E" /></head> <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph ↵p5/cgi </td></tr> <h2>PHP Variables</h2> http://192.168.29.195/phpinfo.php Concluded from: <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV ↵E" /></head> <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph ↵p5/cgi </td></tr> <h2>PHP Variables</h2></div></div>
<div><div>Impact</div><div>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.</div></div>
<div><div>Solution:</div><div><div>Solution type: Workaround</div><div>Delete the listed files or restrict access to them.</div></div></div>
<div><div>Affected Software/OS</div><div>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</div></div>
<div><div>Vulnerability Insight</div><div>... continues on next page ...</div></div>

...continued from previous page ...
Many PHP installation tutorials instruct the user to create a file called <code>phpinfo.php</code> or similar containing the <code>phpinfo()</code> statement. Such a file is often left back in the webserver directory.
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: <code>phpinfo()</code> Output Reporting (HTTP) OID:1.3.6.1.4.1.25623.1.0.11229 Version used: 2025-04-10T05:39:37Z
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

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://192.168.29.195/mutillidae/index.php?page=../../../../../../../../etc/passwd%00</code> ↪ <code>../../../../../../../../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
... continues on next page ...

...continued from previous page ...

url: <http://www.securityfocus.com/bid/12163>

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://192.168.29.195/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

Referencesurl: <https://www.exploit-db.com/exploits/36047/>url: <http://www.securityfocus.com/bid/49187>

Medium (CVSS: 5.0)

NVT: /doc directory browsable

... continues on next page ...

...continued from previous page ...
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://192.168.29.195/doc/
Solution: Solution type: Mitigation Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf: <pre><Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory></pre>
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
References cve: CVE-1999-0678 url: http://www.securityfocus.com/bid/318

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): http://192.168.29.195/dvwa/login.php :password http://192.168.29.195/phpMyAdmin/ :pma_password http://192.168.29.195/phpMyAdmin/?D=A:pma_password http://192.168.29.195/tikiwiki/tiki-install.php :pass http://192.168.29.195/twiki/bin/view/TWiki/TWikiUserAuthentication :oldpassword
Impact ... continues on next page ...

...continued from previous page ...
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.
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.
Affected Software/OS Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
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
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

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):
... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - Identified file: <code>http://192.168.29.195/mutillidae/javascript/ddsmoothmenu/jque↵ry.min.js</code> - Referenced at: <code>http://192.168.29.195/mutillidae/</code>
Solution: Solution type: VendorFix Update to version 1.6.3 or later.
Affected Software/OS jQuery prior to version 1.6.3.
Vulnerability Insight Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using <code>location.hash</code> 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

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
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)
Summary Apache HTTP Server is prone to a cookie information disclosure vulnerability.
Quality of Detection (QoD): 99%
Vulnerability Detection Result
... continues on next page ...

...continued from previous page ...
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 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
... continues on next page ...

...	...continued from previous page ...
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: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
Summary phpMyAdmin is prone to a cross-site scripting (XSS) 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 inject arbitrary HTML code within the error page and conduct phishing attacks.
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 phpMyAdmin version 3.3.8.1 and prior.
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.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page...
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
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

[\[return to 192.168.29.195 \]](#)

2.1.22 Medium 23/tcp

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

[\[return to 192.168.29.195 \]](#)

2.1.23 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.
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

[\[return to 192.168.29.195 \]](#)

2.1.24 Medium 5432/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites
Product detection result cpe:/a:ietf:transport_layer_security
... continues on next page ...

...continued from previous page ...
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↔802067)
Summary This routine reports all weak SSL/TLS cipher suites accepted by a service.
Quality of Detection (QoD): 98%
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
Impact This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.
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.
Affected Software/OS All services providing an encrypted communication using weak SSL/TLS cipher suites.
Vulnerability Insight These rules are applied for the evaluation of the cryptographic strength: - 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
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
... continues on next page ...

...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-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/TechGuidel
 ↪ines/TG02102/BSI-TR-02102-1.html](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](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/Technisch
 ↪eRichtlinien/TR03116/BSI-TR-03116-4.html](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](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](https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters↪-report-2014)
 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 ...

...continued from previous page ...

```

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

```

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 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).

Impact

... continues on next page ...

...continued from previous page ...
<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:</p> <p>Solution type: Mitigation</p> <p>It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Affected Software/OS</p> <p>All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.</p>
<p>Vulnerability Insight</p> <p>The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> - CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE) - CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)
<p>Vulnerability Detection Method</p> <p>Checks the used SSL protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.111012</p> <p>Version used: 2025-03-27T05:38:50Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:ietf:transport_layer_security:1.0</p> <p>Method: SSL/TLS: Version Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p>References</p> <p>cve: CVE-2016-0800</p> <p>cve: CVE-2014-3566</p> <p>url: https://ssl-config.mozilla.org</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel ines/TG02102/BSI-TR-02102-1.html</p> <p>url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/ TLSTLS-Protokoll/TLS-Protokoll_node.html</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch eRichtlinien/TR03116/BSI-TR-03116-4.html</p> <p>url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mind eststandard_BSI_TLS_Version_2_4.html</p> <p>url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org</p> <p>url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</p>
...continues on next page ...

...continued from previous page ...

↔-report-2014
url: <https://drownattack.com>
url: <https://www.imperialviolet.org/2014/10/14/poodle.html>
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
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078

... continues on next page ...

...continued from previous page ...

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
 dfn-cert: DFN-CERT-2015-0396
 dfn-cert: DFN-CERT-2015-0259

...continues on next page ...

...continued from previous page...	
dfn-cert:	DFN-CERT-2015-0254
dfn-cert:	DFN-CERT-2015-0245
dfn-cert:	DFN-CERT-2015-0118
dfn-cert:	DFN-CERT-2015-0114
dfn-cert:	DFN-CERT-2015-0083
dfn-cert:	DFN-CERT-2015-0082
dfn-cert:	DFN-CERT-2015-0081
dfn-cert:	DFN-CERT-2015-0076
dfn-cert:	DFN-CERT-2014-1717
dfn-cert:	DFN-CERT-2014-1680
dfn-cert:	DFN-CERT-2014-1632
dfn-cert:	DFN-CERT-2014-1564
dfn-cert:	DFN-CERT-2014-1542
dfn-cert:	DFN-CERT-2014-1414
dfn-cert:	DFN-CERT-2014-1366
dfn-cert:	DFN-CERT-2014-1354

Medium (CVSS: 5.3)

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

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

Vulnerability Insight

...continues on next page...

...continued from previous page ...
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: 1.3.6.1.4.1.25623.1.0.103692)
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,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX public key algorithm RSA public key size (bits) 1024 serial 00FAF93A4C7FB6B9CC signature algorithm sha1WithRSAEncryption subject 1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX
...continues on next page ...

...continued from previous page ...	
subject alternative names (SAN)	None
valid from	2010-03-17 14:07:45 UTC
valid until	2010-04-16 14:07:45 UTC
Solution: Solution type: Mitigation Replace the SSL/TLS certificate by a new one.	
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.	
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	
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)	

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	
... continues on next page ...	

...continued from previous page ...
<p>Users should contact their vendors for specific patch information.</p> <p>A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.</p>
<p>Affected Software/OS</p> <p>Every SSL/TLS service which does not properly restrict client-initiated renegotiation.</p>
<p>Vulnerability Insight</p> <p>The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.</p> <p>Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:</p> <p>> 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.</p> <p>Both CVEs are still kept in this VT as a reference to the origin of this flaw.</p>
<p>Vulnerability Detection Method</p> <p>Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.</p> <p>Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)</p> <p>OID:1.3.6.1.4.1.25623.1.0.117761</p> <p>Version used: 2024-09-27T05:05:23Z</p>
<p>References</p> <p>cve: CVE-2011-1473</p> <p>cve: CVE-2011-5094</p> <p>url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</p> <p>url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</p> <p>url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</p> <p>url: https://www.openwall.com/lists/oss-security/2011/07/08/2</p> <p>cert-bund: WID-SEC-2024-1591</p> <p>cert-bund: WID-SEC-2024-0796</p> <p>cert-bund: WID-SEC-2023-1435</p> <p>cert-bund: CB-K17/0980</p> <p>cert-bund: CB-K17/0979</p> <p>cert-bund: CB-K14/0772</p> <p>cert-bund: CB-K13/0915</p> <p>cert-bund: CB-K13/0462</p> <p>dfn-cert: DFN-CERT-2025-0933</p> <p>dfn-cert: DFN-CERT-2017-1013</p> <p>dfn-cert: DFN-CERT-2017-1012</p> <p>dfn-cert: DFN-CERT-2014-0809</p> <p>dfn-cert: DFN-CERT-2013-1928</p> <p>dfn-cert: DFN-CERT-2012-1112</p>

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) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
<p>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 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/TechGuidel ↪ines/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/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://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-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</p>
...continues on next page ...

...continued from previous page ...

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
 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

...continues on next page ...

...continued from previous page ...

```

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

... continues on next page ...

...continued from previous page ...
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.
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 Vulnerabili. ↪.. OID:1.3.6.1.4.1.25623.1.0.106223 Version used: 2025-03-27T05:38:50Z
References 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/Mindeststandards_node.html
...continues on next page ...

...continued from previous page ...
<div>↪tstandard_BSI_TLS_Version_2_4.html</div> <div>url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org</div> <div>url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</div> <div>↪-report-2014</div> <div>url: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile</div>
Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
<div>Summary</div> <div>The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.</div>
Quality of Detection (QoD): 80%
<div>Vulnerability Detection Result</div> <div>The following certificates are part of the certificate chain but using insecure ↪signature algorithms:</div> <div>Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173</div> <div>↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic</div> <div>↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi</div> <div>↪ng outside US,C=XX</div> <div>Signature Algorithm: sha1WithRSAEncryption</div>
<div>Solution:</div> <div>Solution type: Mitigation</div> <div>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.</div>
<div>Vulnerability Insight</div> <div>The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:</div> <div>- Secure Hash Algorithm 1 (SHA-1)</div> <div>- Message Digest 5 (MD5)</div> <div>- Message Digest 4 (MD4)</div> <div>- Message Digest 2 (MD2)</div> <div>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.</div> <div>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:</div> <div>Fingerprint1</div> <div>... continues on next page ...</div>

...continued from previous page ...
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 192.168.29.195](#)]

2.1.25 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 ↵4f70656e564153565432303637325f -c50 192.168.29.114’’ on the remote host. Received answer (ICMP "Data" field): 0x00: 6E E0 30 68 74 3E 04 00 56 54 32 30 36 37 32 5F n.0ht>..VT20672_ 0x10: 5F 4F 70 65 6E 56 41 53 56 54 32 30 36 37 32 5F _OpenVASVT20672_ 0x20: 5F 4F 70 65 6E 56 41 53 56 54 32 30 36 37 32 5F _OpenVASVT20672_ 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.
... continues on next page ...

...continued from previous page ...
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.
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

[\[return to 192.168.29.195 \]](#)

2.1.26 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 ... continues on next page ...

...continued from previous page ...
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 Stand ↪ard (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 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6
Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) 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 key exchange (KEX) algorithm(s).											
Quality of Detection (QoD): 80%											
Vulnerability Detection Result The remote SSH server supports the following weak KEX algorithm(s): <table> <thead> <tr> <th>KEX algorithm</th><th>Reason</th></tr> </thead> <tbody> <tr> <td colspan="2">-----</td></tr> <tr> <td colspan="2">↔-----</td></tr> <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										
Impact An attacker can quickly break individual connections.											
Solution: Solution type: Mitigation Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.											
Vulnerability Insight - 1024-bit MODP group / prime KEX algorithms: Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime. A nation-state can break a 1024-bit prime.											
Vulnerability Detection Method Checks the supported KEX algorithms of the remote SSH server. Currently weak KEX algorithms are defined as the following: - non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime - ephemeral generated key exchange groups uses SHA-1 - using RSA 1024-bit modulus key Details: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.150713 Version used: 2024-06-14T05:05:48Z											
Product Detection Result Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)											
... continues on next page ...											

...continued from previous page ...

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
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The remote SSH server supports the following weak server-to-client encryption algorithms:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc

... continues on next page ...

...continued from previous page...	
cast128-cbc rijndael-cbc@lysator.liu.se	
Solution: Solution type: Mitigation Disable the reported weak encryption algorithm(s).	
Vulnerability Insight - 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.	
Vulnerability Detection Method Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak encryption algorithms are defined as the following: - Arcfour (RC4) cipher based algorithms - 'none' algorithm - CBC mode cipher based algorithms 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	
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/rfc8758 url: https://www.kb.cert.org/vuls/id/958563 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3	

[[return to 192.168.29.195](#)]

2.1.27 Low 25/tcp

Low (CVSS: 3.7)
NVT: SSL/TLS: 'DHE_EXPORT' MITM Security Bypass Vulnerability (LogJam)
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↵802067)
Summary This host is accepting 'DHE_EXPORT' cipher suites and is prone to a man-in-the-middle (MITM) vulnerability.
Quality of Detection (QoD): 80%
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
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.
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.
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.
Vulnerability Insight Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
<p>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</p>
<p>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)</p>
<p>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/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/Mindeststandard_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: CB-K21/0067 cert-bund: CB-K19/0812 cert-bund: CB-K16/1593 cert-bund: CB-K16/1552 cert-bund: CB-K16/0617 cert-bund: CB-K16/0599 cert-bund: CB-K16/0168 cert-bund: CB-K16/0121 cert-bund: CB-K16/0090 cert-bund: CB-K16/0030 cert-bund: CB-K15/1591 cert-bund: CB-K15/1550 cert-bund: CB-K15/1517</p>
...continues on next page ...

...continued from previous page ...

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
 dfn-cert: DFN-CERT-2015-1016
 dfn-cert: DFN-CERT-2015-0980
 dfn-cert: DFN-CERT-2015-0977

...continues on next page ...

...continued from previous page ...
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 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.
... continues on next page ...

...continued from previous page ...	
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-ssl-30.html ↪g-ssl-30.html cert-bund: WID-SEC-2023-0431 cert-bund: CB-K17/1198 cert-bund: CB-K17/1196 cert-bund: CB-K16/1828 cert-bund: CB-K16/1438 cert-bund: CB-K16/1384 cert-bund: CB-K16/1102 cert-bund: CB-K16/0599 cert-bund: CB-K16/0156 cert-bund: CB-K15/1514 cert-bund: CB-K15/1358 cert-bund: CB-K15/1021 cert-bund: CB-K15/0972 cert-bund: CB-K15/0637 cert-bund: CB-K15/0590 cert-bund: CB-K15/0525 cert-bund: CB-K15/0393 cert-bund: CB-K15/0384 cert-bund: CB-K15/0287 cert-bund: CB-K15/0252 cert-bund: CB-K15/0246 cert-bund: CB-K15/0237 cert-bund: CB-K15/0118 cert-bund: CB-K15/0110 cert-bund: CB-K15/0108 cert-bund: CB-K15/0080 cert-bund: CB-K15/0078 cert-bund: CB-K15/0077	
... continues on next page ...	

...continued from previous page ...

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
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

[\[return to 192.168.29.195 \]](#)

2.1.28 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: 172707 Packet 2: 172818
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution: 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 ... continues on next page ...

...continued from previous page ...
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

[\[return to 192.168.29.195 \]](#)

2.1.29 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
Vulnerability Insight The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
Vulnerability Detection Method Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190
... continues on next page ...

...continued from previous page ...
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

[\[return to 192.168.29.195 \]](#)

2.1.30 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: <ul style="list-style-type: none"> - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
... continues on next page ...

...continued from previous page...	
Vulnerability Insight	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-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
...continues on next page...	

...continued from previous page ...

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
dfn-cert: DFN-CERT-2014-1632

...continues on next page ...

...continued from previous page ...

```
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
```

[\[return to 192.168.29.195 \]](#)**2.1.31 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
↪)**Summary**

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

Quality of Detection (QoD): 80%**Vulnerability Detection Result**The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):

hmac-md5

hmac-md5-96

hmac-sha1-96

umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):

hmac-md5

hmac-md5-96

hmac-sha1-96

umac-64@openssh.com

Solution:**Solution type:** Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

... continues on next page ...

...continued from previous page ...
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2024-06-14T05:05:48Z
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/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[\[return to 192.168.29.195 \]](#)

2.1.32 Log 8009/tcp

Log (CVSS: 0.0) NVT: Apache JServ Protocol (AJP) v1.3 Detection
Summary The script detects a service supporting the Apache JServ Protocol (AJP) version 1.3.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A service supporting the Apache JServ Protocol (AJP) v1.3 seems to be running on ↪ this port.
Solution:
Log Method Details: Apache JServ Protocol (AJP) v1.3 Detection OID:1.3.6.1.4.1.25623.1.0.108082 Version used: 2023-07-25T05:05:58Z

[\[return to 192.168.29.195 \]](#)

2.1.33 Log 514/tcp

Log (CVSS: 0.0)
NVT: rsh Service Detection
<div><div>Summary</div><div>Checks if the remote host is running a rsh service. Note: The reporting takes place in a separate VT 'rsh Unencrypted Cleartext Login' (OID: 1.3.6.1.4.1.25623.1.0.100080).</div></div>
Quality of Detection (QoD): 80%
<div><div>Vulnerability Detection Result</div><div>A rsh service is running at this port.</div></div>
Solution:
<div><div>Log Method</div><div>Details: rsh Service Detection OID:1.3.6.1.4.1.25623.1.0.108478 Version used: 2024-06-26T05:05:39Z</div></div>

[\[return to 192.168.29.195 \]](#)

2.1.34 Log 25/tcp

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection
<div><div>Product detection result</div><div>cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)</div></div>
<div><div>Summary</div><div>The SSL/TLS certificate on this port is self-signed.</div></div>
Quality of Detection (QoD): 98%
... continues on next page ...

...continued from previous page ...	
Vulnerability Detection Result The certificate of the remote service is self signed. Certificate details: fingerprint (SHA-1) ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256) E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A ↪F1E32DEE436DE813CC issued by 1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX public key algorithm RSA public key size (bits) 1024 serial 00FAF93A4C7FB6B9CC signature algorithm sha1WithRSAEncryption subject 1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX subject alternative names (SAN) None valid from 2010-03-17 14:07:45 UTC valid until 2010-04-16 14:07:45 UTC	
Solution:	
Log Method Details: SSL/TLS: Certificate - Self-Signed Certificate Detection OID:1.3.6.1.4.1.25623.1.0.103140 Version used: 2024-06-14T05:05:48Z	
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)	
References url: http://en.wikipedia.org/wiki/Self-signed_certificate	
Log (CVSS: 0.0)	
NVT: SSL/TLS: SMTP 'STARTTLS' Command Detection	
Summary	
... continues on next page ...	

...continued from previous page ...
Checks if the remote SMTP server supports SSL/TLS with the 'STARTTLS' command.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The remote SMTP server supports SSL/TLS with the 'STARTTLS' command. The remote SMTP server is announcing the following available ESMTP commands (EHL ↪0 response) before sending the 'STARTTLS' command: 8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, V ↪RFY The remote SMTP server is announcing the following available ESMTP commands (EHL ↪0 response) after sending the 'STARTTLS' command: 8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, VRFY
Solution:
Log Method Details: SSL/TLS: SMTP 'STARTTLS' Command Detection OID:1.3.6.1.4.1.25623.1.0.103118 Version used: 2023-10-31T05:06:37Z
References url: https://tools.ietf.org/html/rfc3207

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection
Summary Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The remote SSL/TLS service supports the following SSL/TLS protocol version(s): SSLv2 SSLv3 TLSv1.0
Solution:
Log Method Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
... continues on next page ...

...continued from previous page ...
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers. Details: SSL/TLS: Version Detection OID:1.3.6.1.4.1.25623.1.0.105782 Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0) NVT: Postfix SMTP Server Detection (SMTP)
Summary SMTP based detection of Postfix.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected Postfix Version: unknown Location: 25/tcp CPE: cpe:/a:postfix:postfix Concluded from version/product identification result: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
Solution:
Log Method Details: Postfix SMTP Server Detection (SMTP) OID:1.3.6.1.4.1.25623.1.0.111086 Version used: 2024-01-12T05:05:56Z
References url: https://www.postfix.org/

Log (CVSS: 0.0) NVT: SMTP Server type and version
Summary This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.
Quality of Detection (QoD): 80%
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Remote SMTP server banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu) The remote SMTP server is announcing the following available ESMTP commands (EHL ↪ response) via an unencrypted connection: 8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, V ↪ RFY
Solution:
Log Method Details: SMTP Server type and version OID:1.3.6.1.4.1.25623.1.0.10263 Version used: 2024-09-25T05:06:11Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) 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. ↪ 802067)
Summary This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).
Quality of Detection (QoD): 98%
Vulnerability Detection Result Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv ↪ ice via the SSLv3 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv ↪ ice via the TLSv1.0 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA
... continues on next page ...

...continued from previous page ...
TLS_DHE_RSA_WITH_DES_CBC_SHA
Solution:
Log Method Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites OID:1.3.6.1.4.1.25623.1.0.105018 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)

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium 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.↪802067)
Summary This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Quality of Detection (QoD): 98%
Vulnerability Detection Result 'Medium' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_DH_anon_WITH_3DES_EDE_CBC_SHA TLS_DH_anon_WITH_AES_128_CBC_SHA TLS_DH_anon_WITH_DES_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA 'Medium' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA
... continues on next page ...

...continued from previous page ...
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA TLS_DH_anon_WITH_AES_128_CBC_SHA TLS_DH_anon_WITH_DES_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA
Solution:
Vulnerability Insight Any cipher suite considered to be secure for only the next 10 years is considered as medium.
Log Method Details: SSL/TLS: Report Medium Cipher Suites OID:1.3.6.1.4.1.25623.1.0.902816 Version used: 2024-09-27T05:05:23Z
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)

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non 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.↪802067)
Summary This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.
Quality of Detection (QoD): 98%
Vulnerability Detection Result 'Weak' 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 TLS_DH_anon_WITH_RC4_128_MD5 TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
... continues on next page ...

...continued from previous page...

```

TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' 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
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA

```

Solution:**Log Method**

Details: SSL/TLS: Report Non Weak Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.103441

...continues on next page...

...continued from previous page ...
Version used: 2024-09-27T05:05:23Z
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)

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites
Summary This routine reports all SSL/TLS cipher suites accepted by a service.
Quality of Detection (QoD): 98%
Vulnerability Detection Result 'Strong' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DH_anon_WITH_AES_256_CBC_SHA 'Medium' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_DH_anon_WITH_3DES_EDE_CBC_SHA TLS_DH_anon_WITH_AES_128_CBC_SHA TLS_DH_anon_WITH_DES_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA 'Weak' 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 TLS_DH_anon_WITH_RC4_128_MD5 TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA No 'Null' cipher suites accepted by this service via the SSLv3 protocol. 'Anonymous' cipher suites accepted by this service via the SSLv3 protocol: TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 TLS_DH_anon_WITH_3DES_EDE_CBC_SHA ... continues on next page ...

...continued from previous page...

```

TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' 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
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5

```

Solution:**Vulnerability Insight**

Notes:

- As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead.

...continues on next page...

...continued from previous page ...
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.
Log Method Details: SSL/TLS: Report Supported Cipher Suites OID:1.3.6.1.4.1.25623.1.0.802067 Version used: 2024-09-27T05:05:23Z

Log (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.↵802067)
Summary This routine reports all weak SSL/TLS cipher suites accepted by a service.
Quality of Detection (QoD): 98%
Vulnerability Detection Result 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 c ↵learntext communication. 'Weak' 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 TLS_DH_anon_WITH_RC4_128_MD5 TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA 'Weak' 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 TLS_DH_anon_WITH_RC4_128_MD5 TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 ... continues on next page ...

...continued from previous page ...
TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
Impact This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.
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.
Affected Software/OS All services providing an encrypted communication using weak SSL/TLS cipher suites.
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
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
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-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/TechGuidel
... continues on next page ...

...continued from previous page...

↪ines/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/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>
 cert-bund: CB-K21/0067
 cert-bund: CB-K19/0812
 cert-bund: CB-K17/1750
 cert-bund: CB-K16/1593
 cert-bund: CB-K16/1552
 cert-bund: CB-K16/1102
 cert-bund: CB-K16/0617
 cert-bund: CB-K16/0599
 cert-bund: CB-K16/0168
 cert-bund: CB-K16/0121
 cert-bund: CB-K16/0090
 cert-bund: CB-K16/0030
 cert-bund: CB-K15/1751
 cert-bund: CB-K15/1591
 cert-bund: CB-K15/1550
 cert-bund: CB-K15/1517
 cert-bund: CB-K15/1514
 cert-bund: CB-K15/1464
 cert-bund: CB-K15/1442
 cert-bund: CB-K15/1334
 cert-bund: CB-K15/1269
 cert-bund: CB-K15/1136
 cert-bund: CB-K15/1090
 cert-bund: CB-K15/1059
 cert-bund: CB-K15/1022
 cert-bund: CB-K15/1015
 cert-bund: CB-K15/0986
 cert-bund: CB-K15/0964
 cert-bund: CB-K15/0962
 cert-bund: CB-K15/0932
 cert-bund: CB-K15/0927
 cert-bund: CB-K15/0926
 cert-bund: CB-K15/0907
 cert-bund: CB-K15/0901
 cert-bund: CB-K15/0896
 cert-bund: CB-K15/0889
 cert-bund: CB-K15/0877

...continues on next page...

...continued from previous page ...

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
 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

...continues on next page ...

...continued from previous page ...
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

Log (CVSS: 0.0)

NVT: SSL/TLS: Untrusted Certificate Detection

Summary

Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

The remote SSL/TLS server is using the following certificate(s) which failed the
↪ verification against the system wide trust store (serial:issuer):
00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652
↪E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complicati
↪on of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing
↪outside US,C=XX (Server certificate)

Solution:

Log Method

Details: SSL/TLS: Untrusted Certificate Detection

OID:1.3.6.1.4.1.25623.1.0.117764

Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)

NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary

Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

...continues on next page ...

...continued from previous page ...
<div>Quality of Detection (QoD): 98%</div>
<div><div>Vulnerability Detection Result</div><div>Protocol Version Safe/Secure Renegotiation Support Status</div><div></div><div></div><div>SSLv3 Unknown, Reason: Scanner failed to negotiate an SSL/TLS connection (Either the scanner or the remote host is probably not supporting / accepting this SSL/TLS protocol version).</div><div>TLSv1.0 Enabled, Note: While the remote service announces the support of safe/secure renegotiation it still might not support / accept renegotiation at all.</div><div>TLSv1.1 Unknown, Reason: Scanner failed to negotiate an SSL/TLS connection (Either the scanner or the remote host is probably not supporting / accepting this SSL/TLS protocol version).</div><div>TLSv1.2 Unknown, Reason: Scanner failed to negotiate an SSL/TLS connection (Either the scanner or the remote host is probably not supporting / accepting this SSL/TLS protocol version).</div><div>TLSv1.3 Unknown, Reason: Scanner failed to negotiate an SSL/TLS connection (Either the scanner or the remote host is probably not supporting / accepting this SSL/TLS protocol version).</div></div>
<div>Solution:</div>
<div><div>Log Method</div><div>Details: SSL/TLS: Safe/Secure Renegotiation Support Status</div><div>OID:1.3.6.1.4.1.25623.1.0.117757</div><div>Version used: 2024-09-27T05:05:23Z</div></div>
<div><div>References</div><div>url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html</div><div>url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation</div><div>url: https://datatracker.ietf.org/doc/html/rfc5746</div></div>

<div>Log (CVSS: 0.0)</div>
<div>NVT: Services</div>
<div><div>Summary</div><div>This plugin performs service detection.</div></div>
<div>Quality of Detection (QoD): 80%</div>
<div><div>Vulnerability Detection Result</div><div>... continues on next page ...</div></div>

...continued from previous page ...
An SMTP server is running on this port Here is its banner : 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
Solution:
Vulnerability Insight This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2025-03-05T05:38:53Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details
Summary This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.
Quality of Detection (QoD): 98%
Vulnerability Detection Result The following certificate details of the remote service were collected. Certificate details: fingerprint (SHA-1) ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256) E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A ↪F1E32DEE436DE813CC issued by 1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX public key algorithm RSA public key size (bits) 1024 serial 00FAF93A4C7FB6B9CC signature algorithm sha1WithRSAEncryption subject 1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX subject alternative names (SAN) None
... continues on next page ...

...continued from previous page ...	
valid from	2010-03-17 14:07:45 UTC
valid until	2010-04-16 14:07:45 UTC
Solution:	
Log Method Details: SSL/TLS: Collect and Report Certificate Details OID:1.3.6.1.4.1.25623.1.0.103692 Version used: 2024-09-27T05:05:23Z	

[[return to 192.168.29.195](#)]

2.1.35 Log 3632/tcp

Log (CVSS: 0.0) NVT: DistCC Detection
Summary Tries to detect if the remote host is running a DistCC service.
Quality of Detection (QoD): 95%
Vulnerability Detection Result A DistCC service is running at this port.
Solution:
Log Method Details: DistCC Detection OID:1.3.6.1.4.1.25623.1.0.12638 Version used: 2023-08-01T13:29:10Z

[[return to 192.168.29.195](#)]

2.1.36 Log 5900/tcp

Log (CVSS: 0.0) NVT: VNC Server and Protocol Version Detection (TCP)
... continues on next page ...

...continued from previous page ...
Summary TCP based detection of Virtual Network Computing (VNC) services and the underlying Remote Framebuffer Protocol (RFB) version.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A VNC server seems to be running on this port. The version of the VNC protocol is : RFB 003.003
Solution: Make sure the use of this software is done in accordance with your corporate security policy, filter incoming traffic to this port.
Vulnerability Insight The remote host is running a remote display software (VNC) which permits a console to be displayed remotely. This allows authenticated users of the remote host to take its control remotely.
Log Method Details: VNC Server and Protocol Version Detection (TCP) OID:1.3.6.1.4.1.25623.1.0.10342 Version used: 2025-03-19T05:38:35Z
References url: https://datatracker.ietf.org/doc/html/rfc6143 url: https://datatracker.ietf.org/doc/html/rfc7869

Log (CVSS: 0.0)
NVT: VNC Supported 'security types' Detection (TCP)
Summary TCP based detection of the available remote Virtual Network Computing (VNC) 'security types'.
Quality of Detection (QoD): 95%
Vulnerability Detection Result The remote VNC server chose security type #2 (VNC authentication)
Solution:
Log Method
... continues on next page ...

...continued from previous page ...
Details: VNC Supported 'security types' Detection (TCP) OID:1.3.6.1.4.1.25623.1.0.19288 Version used: 2025-03-19T05:38:35Z
References url: https://datatracker.ietf.org/doc/html/rfc6143 url: https://datatracker.ietf.org/doc/html/rfc7869

[[return to 192.168.29.195](#)]

2.1.37 Log general/tcp

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting
Summary The script reports information on how the hostname of the target was determined.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Hostname determination for IP 192.168.29.195: Hostname Source 192.168.29.195 IP-address
Solution:
Log Method Details: Hostname Determination Reporting OID:1.3.6.1.4.1.25623.1.0.108449 Version used: 2022-07-27T10:11:28Z

Log (CVSS: 0.0)
NVT: Traceroute
Summary Collect information about the network route and network distance between the scanner host and the target host.
Quality of Detection (QoD): 80%
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Network route from scanner (192.168.29.114) to target (192.168.29.195): 192.168.29.114 192.168.29.195 Network distance between scanner and target: 2
Solution:
Vulnerability Insight For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.
Log Method A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'. Details: Traceroute OID:1.3.6.1.4.1.25623.1.0.51662 Version used: 2022-10-17T11:13:19Z

Log (CVSS: 0.0)
NVT: jQuery Detection Consolidation
Summary Consolidation of jQuery detections.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected jQuery Version: 1.3.2 Location: /mutillidae/javascript/ddsmoothmenu/jquery.min.js CPE: cpe:/a:jquery:jquery:1.3.2 Concluded from version/product identification result: src="/javascript/ddsmoothmenu/jquery.min.js jQuery JavaScript Library v1.3.2 Concluded from version/product identification location: - Identified file: http://192.168.29.195/mutillidae/javascript/ddsmoothmenu/jque ↳ ry.min.js - Referenced at: http://192.168.29.195/mutillidae/
Solution:
... continues on next page ...

...continued from previous page ...
Log Method Details: jQuery Detection Consolidation OID:1.3.6.1.4.1.25623.1.0.150658 Version used: 2023-07-14T05:06:08Z
References url: https://jquery.com/

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate
Summary It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.
Quality of Detection (QoD): 98%
Vulnerability Detection Result The following additional but not resolvable hostnames were detected: ubuntu804-base.localdomain
Solution:
Log Method Details: SSL/TLS: Hostname discovery from server certificate OID:1.3.6.1.4.1.25623.1.0.111010 Version used: 2021-11-22T15:32:39Z

Log (CVSS: 0.0)
NVT: Apache HTTP Server Detection Consolidation
Summary Consolidation of Apache HTTP Server detections.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected Apache HTTP Server Version: 2.2.8 Location: 80/tcp CPE: cpe:/a:apache:http_server:2.2.8
... continues on next page ...

...continued from previous page ...
Concluded from version/product identification result: Server: Apache/2.2.8 (Ubuntu) DAV/2
Solution:
Log Method Details: Apache HTTP Server Detection Consolidation OID:1.3.6.1.4.1.25623.1.0.117232 Version used: 2024-03-08T15:37:10Z
References url: https://httpd.apache.org

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting
Summary This script consolidates the OS information detected by several VTs and tries to find the best matching OS. Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection. If any of this information is wrong or could be improved please consider to report these to the referenced community forum.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Best matching OS: OS: Ubuntu 8.04 Version: 8.04 CPE: cpe:/o:canonical:ubuntu_linux:8.04 Found by VT: 1.3.6.1.4.1.25623.1.0.105586 (Operating System (OS) Detection (SSH ⇄ Banner)) Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 Setting key "Host/runs_unixoide" based on this information Other OS detections (in order of reliability): OS: Linux/Unix CPE: cpe:/o:linux:kernel Found by VT: 1.3.6.1.4.1.25623.1.0.105355 (Operating System (OS) Detection (FTP ⇄)) Concluded from FTP banner on port 21/tcp: 220 (vsFTPd 2.3.4) OS: Debian GNU/Linux CPE: cpe:/o:debian:debian_linux Found by VT: 1.3.6.1.4.1.25623.1.0.105355 (Operating System (OS) Detection (FTP ... continues on next page ...

[illegible]

...continued from previous page...
Found by VT: 1.3.6.1.4.1.25623.1.0.108192 (Operating System (OS) Detection (MySQL/MariaDB)) Concluded from MySQL/MariaDB server banner on port 3306/tcp: 5.0.51a-3ubuntu5
Solution:
Log Method Details: OS Detection Consolidation and Reporting OID:1.3.6.1.4.1.25623.1.0.105937 Version used: 2025-05-22T05:40:21Z
References url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: OpenSSH Detection Consolidation
Summary Consolidation of OpenSSH detections.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected OpenSSH Server Version: 4.7p1 Location: 22/tcp CPE: cpe:/a:openbsd:openssh:4.7p1 Concluded from version/product identification result: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Solution:
Log Method Details: OpenSSH Detection Consolidation OID:1.3.6.1.4.1.25623.1.0.108577 Version used: 2024-12-13T05:05:32Z
References url: https://www.openssh.com/

Log (CVSS: 0.0)
NVT: ISC BIND Detection Consolidation
Summary Consolidation of ISC BIND detections.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected ISC BIND Version: 9.4.2 Location: 53/tcp CPE: cpe:/a:isc:bind:9.4.2 Concluded from version/product identification result: 9.4.2
Solution:
Log Method Details: ISC BIND Detection Consolidation OID:1.3.6.1.4.1.25623.1.0.145294 Version used: 2022-03-28T10:48:38Z
References url: https://www.isc.org/bind/

Log (CVSS: 0.0)
NVT: PostgreSQL Detection Consolidation
Summary Consolidation of PostgreSQL detections.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected PostgreSQL Version: 8.3.1 Location: 5432/tcp CPE: cpe:/a:postgresql:postgresql:8.3.1 Concluded from version/product identification result: select version(); query result: T versionDg]PostgreSQL 8.3.1 on i486-pc-linux-gn ↪u, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)CSELECTZI
... continues on next page ...

...continued from previous page ...
Solution:
Log Method Details: PostgreSQL Detection Consolidation OID:1.3.6.1.4.1.25623.1.0.128025 Version used: 2024-07-19T05:05:32Z
References url: https://www.postgresql.org/

[\[return to 192.168.29.195 \]](#)

2.1.38 Log 21/tcp

Log (CVSS: 0.0) NVT: FTP Banner Detection
Summary This script detects and reports a FTP Server Banner.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Remote FTP server banner: 220 (vsFTPd 2.3.4) This is probably (a): - vsFTPd Server operating system information collected via "SYST" command: 215 UNIX Type: L8 Server status information collected via "STAT" command: 211-FTP server status: Connected to 192.168.29.114 Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 300 Control connection is plain text Data connections will be plain text vsFTPd 2.3.4 - secure, fast, stable 211 End of status
Solution:
... continues on next page ...

...continued from previous page ...

Log Method

Details: FTP Banner Detection

OID:1.3.6.1.4.1.25623.1.0.10092

Version used: 2025-04-16T05:39:43Z

Log (CVSS: 0.0)

NVT: vsFTPD FTP Server Detection

Summary

The script is grabbing the banner of a FTP server and attempts to identify a vsFTPD FTP Server and its version from the reply.

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

Detected vsFTPD

Version: 2.3.4

Location: 21/tcp

CPE: cpe:/a:beasts:vsftpd:2.3.4

Concluded from version/product identification result:
220 (vsFTPD 2.3.4)

Solution:**Log Method**

Details: vsFTPD FTP Server Detection

OID:1.3.6.1.4.1.25623.1.0.111050

Version used: 2023-07-26T05:05:09Z

Log (CVSS: 0.0)

NVT: SSL/TLS: FTP Missing Support For AUTH TLS

Summary

The remote FTP server does not support the 'AUTH TLS' command.

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

The remote FTP server does not support the 'AUTH TLS' command.

... continues on next page ...

...continued from previous page ...
Solution:
Log Method Details: SSL/TLS: FTP Missing Support For AUTH TLS OID:1.3.6.1.4.1.25623.1.0.108553 Version used: 2021-03-19T08:13:38Z

Log (CVSS: 0.0)
NVT: Services
Summary This plugin performs service detection.
Quality of Detection (QoD): 80%
Vulnerability Detection Result An FTP server is running on this port. Here is its banner : 220 (vsFTPd 2.3.4)
Solution:
Vulnerability Insight This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2025-03-05T05:38:53Z

[\[return to 192.168.29.195 \]](#)

2.1.39 Log 80/tcp

Log (CVSS: 0.0)
NVT: phpMyAdmin Detection (HTTP)
... continues on next page ...

...continued from previous page ...
Summary HTTP based detection of phpMyAdmin.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected phpMyAdmin Version: 3.1.1 Location: /phpMyAdmin CPE: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Concluded from version/product identification result: Version 3.1.1 Concluded from version/product identification location: http://192.168.29.195/phpMyAdmin/index.php http://192.168.29.195/phpMyAdmin/README Extra information: - Protected by Username/Password
Solution:
Log Method Details: phpMyAdmin Detection (HTTP) OID:1.3.6.1.4.1.25623.1.0.900129 Version used: 2024-02-19T14:37:31Z

Log (CVSS: 0.0)
NVT: HTTP Server type and version
Summary This script detects and reports the HTTP Server's banner which might provide the type and version of it.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The remote HTTP Server banner is: Server: Apache/2.2.8 (Ubuntu) DAV/2
Solution:
Log Method Details: HTTP Server type and version OID:1.3.6.1.4.1.25623.1.0.10107
... continues on next page ...

...continued from previous page ...
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration
Summary This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).
Quality of Detection (QoD): 80%
Vulnerability Detection Result It was possible to enumerate the following HTTP server banner(s): Server banner Enumeration technique ----- ↪----- Server: Apache/2.2.8 (Ubuntu) DAV/2 Invalid HTTP 00.5 GET request (non-existent ↪t HTTP version) to '/' X-Powered-By: PHP/5.2.4-2ubuntu5.10 Invalid HTTP 00.5 GET request (non-existent ↪t HTTP version) to '/'
Solution:
Log Method Details: HTTP Server Banner Enumeration OID:1.3.6.1.4.1.25623.1.0.108708 Version used: 2025-01-31T15:39:24Z

Log (CVSS: 0.0)
NVT: 'favicon.ico' Based Fingerprinting (HTTP)
Summary HTTP based fingerprinting of web applications based on an exposed 'favicon.ico' file.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The following apps/services were identified: "phpmyadmin (2.11.8.1 - 4.2.x)" fingerprinted by the file: "http://192.168.29.19 ↪5/phpMyAdmin/favicon.ico"
... continues on next page ...

...continued from previous page ...

Solution:**Log Method**

Details: 'favicon.ico' Based Fingerprinting (HTTP)

OID:1.3.6.1.4.1.25623.1.0.20108

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

Log (CVSS: 0.0)

NVT: HTTP Security Headers Detection

Summary

All known security headers are being checked on the remote web server.

On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

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

Missing Headers | More Information

```

-----
↪-----
↪-----
Content-Security-Policy | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo

```

... continues on next page ...

...continued from previous page...	
↳rted only in newer browsers like e.g. Firefox 90	
Sec-Fetch-Site	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers , Note: This is a new header supported only in newer browsers like e.g. Firefox 90
Sec-Fetch-User	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers , Note: This is a new header supported only in newer browsers like e.g. Firefox 90
X-Content-Type-Options	https://owasp.org/www-project-secure-headers/#x-content-type-options
X-Frame-Options	https://owasp.org/www-project-secure-headers/#x-frame-options
X-Permitted-Cross-Domain-Policies	https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies
X-XSS-Protection	https://owasp.org/www-project-secure-headers/#x-xss-protection , Note: Most major browsers have dropped / deprecated support for this header in 2020.
Solution:	
Log Method Details: HTTP Security Headers Detection OID:1.3.6.1.4.1.25623.1.0.112081 Version used: 2025-03-21T15:40:43Z	
References url: https://owasp.org/www-project-secure-headers/ url: https://owasp.org/www-project-secure-headers/#div-headers url: https://securityheaders.com/	

Log (CVSS: 0.0)	
NVT: TWiki Version Detection	
Summary Detection of TWiki. The script sends a HTTP connection request to the server and attempts to detect the presence of TWiki and to extract its version.	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result Detected TWiki Version: 01.Feb.2003 Location: /twiki/bin CPE: cpe:/a:twiki:twiki:01.Feb.2003	
... continues on next page ...	

...continued from previous page ...
Concluded from version/product identification result: This site is running Twiki version 01 Feb 2003
Solution:
Log Method Details: Twiki Version Detection OID:1.3.6.1.4.1.25623.1.0.800399 Version used: 2023-07-25T05:05:58Z

Log (CVSS: 0.0)
NVT: Services
Summary This plugin performs service detection.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A web server is running on this port
Solution:
Vulnerability Insight This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2025-03-05T05:38:53Z

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting
Summary The script consolidates and reports various information for web application (formerly called 'CGI') scanning. This information is based on the following scripts / settings:
... continues on next page ...

<p>...continued from previous page ...</p> <ul style="list-style-type: none"> - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use <p>If you think any of this information is wrong please report it to the referenced community forum.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>The Hostname/IP "192.168.29.195" was used to access the remote host. Generic web application scanning is disabled for this host via the "Enable gener ic web application scanning" option within the "Global variable settings" of t he scan config in use.</p> <p>Requests to this service are done via HTTP/1.1. This service seems to be able to host PHP scripts. This service seems to be able to host ASP scripts. The User-Agent "Mozilla/5.0 [en] (X11; U; OpenVAS-VT 23.19.0)" was used to acces s the remote host.</p> <p>Historic /scripts and /cgi-bin are not added to the directories used for web app lication scanning. You can enable this again with the "Add historic /scripts a nd /cgi-bin to directories for CGI scanning" option within the "Global variabl e settings" of the scan config in use.</p> <p>A possible recursion was detected during web application scanning: The service is using a relative URL in one or more HTML references where e.g. /f ile1.html contains and a subsequent request for s ubdir/file2.html is linking to subdir/file2.html. This would resolves to subdi r/subdir/file2.html causing a recursion. To work around this counter-measures have been enabled but the service should be fixed as well to not use such prob lematic links. Below an excerpt of URLs is shown to help identify those issues .</p> <p>Syntax : URL (HTML link) http://192.168.29.195/mutillidae/index.php (index.php?page=documentation/how-to- access-Mutillidae-over-Virtual-Box-network.php) http://192.168.29.195/mutillidae/index.php (index.php?page=documentation/vulnera bilities.php)</p> <p>The following directories were used for web application scanning: http://192.168.29.195/ http://192.168.29.195/cgi-bin http://192.168.29.195/dav http://192.168.29.195/doc http://192.168.29.195/dvwa http://192.168.29.195/index http://192.168.29.195/index/ajax</p> <p>... continues on next page ...</p>

...continued from previous page...

```

http://192.168.29.195/index/download
http://192.168.29.195/mutillidae
http://192.168.29.195/mutillidae/documentation
http://192.168.29.195/oops/TWiki
http://192.168.29.195/phpMyAdmin
http://192.168.29.195/rdiff/TWiki
http://192.168.29.195/test
http://192.168.29.195/test/testoutput
http://192.168.29.195/tikiwiki
http://192.168.29.195/tikiwiki/lib
http://192.168.29.195/twiki
http://192.168.29.195/twiki/pub
http://192.168.29.195/twiki/pub/TWiki/FileAttachment
http://192.168.29.195/twiki/pub/TWiki/TWikiDocGraphics
http://192.168.29.195/twiki/pub/TWiki/TWikiLogos
http://192.168.29.195/twiki/pub/TWiki/TWikiPreferences
http://192.168.29.195/twiki/pub/TWiki/TWikiTemplates
http://192.168.29.195/twiki/pub/icn
http://192.168.29.195/view/TWiki
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from web application scanning because th
↪e "Regex pattern to exclude directories from CGI scanning" setting of the VT "
↪Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was
↪: "/(index\.php|image|img|css|js$|js|/|javascript|style|theme|icon|jquery|graph
↪ic|grafik|picture|bilder|thumbnail|media/|skins?/)"
http://192.168.29.195/dvwa/dvwa/css
http://192.168.29.195/dvwa/dvwa/images
http://192.168.29.195/icons
http://192.168.29.195/index.php/Home
http://192.168.29.195/index.php/Home/login
http://192.168.29.195/index.php/installer
http://192.168.29.195/index.php/s
http://192.168.29.195/index.php/wp-json
http://192.168.29.195/mutillidae/images
http://192.168.29.195/mutillidae/javascript
http://192.168.29.195/mutillidae/javascript/ddsmoothmenu
http://192.168.29.195/mutillidae/styles
http://192.168.29.195/mutillidae/styles/ddsmoothmenu
http://192.168.29.195/phpMyAdmin/themes/original/img
http://192.168.29.195/tikiwiki/img/icons
http://192.168.29.195/tikiwiki/styles
http://192.168.29.195/tikiwiki/styles/transitions
Directory index found at:
http://192.168.29.195/dav/
http://192.168.29.195/mutillidae/documentation/
...continues on next page ...

```

...continued from previous page...

```

http://192.168.29.195/test/
http://192.168.29.195/test/testoutput/
http://192.168.29.195/twiki/TWikiDocumentation.html
http://192.168.29.195/twiki/bin/view/TWiki/TWikiDocumentation
http://192.168.29.195/twiki/bin/view/TWiki/TWikiInstallationGuide
Extraneous phpinfo() output found at:
http://192.168.29.195/mutillidae/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
  ↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
  ↪p5/cgi </td></tr>
  <h2>PHP Variables</h2>
http://192.168.29.195/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
  ↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
  ↪p5/cgi </td></tr>
  <h2>PHP Variables</h2>
PHP script discloses physical path at:
http://192.168.29.195/mutillidae/documentation/vulnerabilities.php (/var/www/mut
  ↪illidae/documentation/vulnerabilities.php)
http://192.168.29.195/tikiwiki/tiki-install.php (/var/www/tikiwiki/lib/adodb/dri
  ↪vers/adodb-mysql.inc.php)
The "Number of pages to mirror" setting (Current: 200) of the VT "Web mirroring"
  ↪ (OID: 1.3.6.1.4.1.25623.1.0.10662) was reached. Raising this limit allows to
  ↪mirror this host more thoroughly but might increase the scanning time.
NOTE: The 'Maximum number of items shown for each list' setting has been reached
  ↪. There are 355 additional entries available for the following truncated list.
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://192.168.29.195/dav/ (C=S;0 [A] C=N;0 [D] C=M;0 [A] C=D;0 [A] )
http://192.168.29.195/dvwa/login.php (username [] password [] Login [Login] )
http://192.168.29.195/mutillidae/ (page [add-to-your-blog.php] )
http://192.168.29.195/mutillidae/documentation/ (C=S;0 [A] C=N;0 [D] C=M;0 [A] C
  ↪=D;0 [A] )
http://192.168.29.195/mutillidae/index.php (username [anonymous] do [toggle-hint
  ↪s] page [home.php] )
http://192.168.29.195/oops/TWiki/TWikiHistory (template [oopsrev] param1 [1.10]
  ↪)
http://192.168.29.195/phpMyAdmin/index.php (phpMyAdmin [0af2f7f6c4a0883fc0b3eb58
  ↪9595bec0a444a879] token [***replaced***] pma_username [] table [] lang [] serv
  ↪er [1] db [] convcharset [utf-8] pma_password [] )
http://192.168.29.195/phpMyAdmin/phpmyadmin.css.php (token [***replaced***] js_f
  ↪rame [right] lang [en-utf-8] nocache [2457687151] convcharset [utf-8] )
http://192.168.29.195/rdiff/TWiki/TWikiHistory (rev1 [1.10] rev2 [1.9] )
...continues on next page ...

```

...continued from previous page...

```

http://192.168.29.195/test/ (C=S;0 [A] C=N;0 [D] C=M;0 [A] C=D;0 [A] )
http://192.168.29.195/test/testoutput/ (C=S;0 [A] C=N;0 [D] C=M;0 [A] C=D;0 [A]
↔)
http://192.168.29.195/tikiwiki/tiki-install.php (host [localhost] dbinfo [] pass
↔ [] name [] db [] restart [1] resetdb [] user [] )
http://192.168.29.195/twiki/bin/attach/TWiki/FileAttachment (filename [Sample.tx
↔t] revInfo [1] )
http://192.168.29.195/twiki/bin/edit/Know/ReadmeFirst (t [1748033245] )
http://192.168.29.195/twiki/bin/edit/Know/WebChanges (t [1748033149] )
http://192.168.29.195/twiki/bin/edit/Know/WebHome (t [1748033126] )
http://192.168.29.195/twiki/bin/edit/Know/WebIndex (t [1748033246] )
http://192.168.29.195/twiki/bin/edit/Know/WebNotify (t [1748033247] )
http://192.168.29.195/twiki/bin/edit/Know/WebPreferences (t [1748033154] )
http://192.168.29.195/twiki/bin/edit/Know/WebSearch (t [1748033153] )
http://192.168.29.195/twiki/bin/edit/Know/WebStatistics (t [1748033248] )
http://192.168.29.195/twiki/bin/edit/Know/WebTopicList (t [1748033247] )
http://192.168.29.195/twiki/bin/edit/Main/BillClinton (topicparent [Main.TWikiUs
↔ers] )
http://192.168.29.195/twiki/bin/edit/Main/CharleytheHorse (t [1748033256] )
http://192.168.29.195/twiki/bin/edit/Main/ChristopheVermeulen (topicparent [Main
↔.TWikiUsers] )
http://192.168.29.195/twiki/bin/edit/Main/DavidWarman (topicparent [Main.TWikiUs
↔ers] )
http://192.168.29.195/twiki/bin/edit/Main/EngineeringGroup (topicparent [Main.TW
↔ikiGroups] )
http://192.168.29.195/twiki/bin/edit/Main/GoodStyle (topicparent [Main.WebHome]
↔)
http://192.168.29.195/twiki/bin/edit/Main/JohnAltstadt (topicparent [Main.TWikiU
↔sers] )
http://192.168.29.195/twiki/bin/edit/Main/JohnTalintyre (t [1748033257] )
http://192.168.29.195/twiki/bin/edit/Main/MartinRaabe (topicparent [TWiki.TWikiU
↔pgradeGuide] )
http://192.168.29.195/twiki/bin/edit/Main/NicholasLee (t [1748033257] )
http://192.168.29.195/twiki/bin/edit/Main/OfficeLocations (t [1748033131] )
http://192.168.29.195/twiki/bin/edit/Main/PeterFokkinga (topicparent [Main.TWiki
↔Users] )
http://192.168.29.195/twiki/bin/edit/Main/PeterThoeny (t [1748033189] )
http://192.168.29.195/twiki/bin/edit/Main/SupportGroup (topicparent [Main.TWikiG
↔roups] )
http://192.168.29.195/twiki/bin/edit/Main/TWikiAdminGroup (t [1748033260] )
http://192.168.29.195/twiki/bin/edit/Main/TWikiGroups (t [1748033130] )
http://192.168.29.195/twiki/bin/edit/Main/TWikiGuest (t [1748033258] )
http://192.168.29.195/twiki/bin/edit/Main/TWikiPreferences (topicparent [Main.We
↔bHome] )
http://192.168.29.195/twiki/bin/edit/Main/TWikiRegistration (topicparent [Main.T
↔WikiUsers] )
http://192.168.29.195/twiki/bin/edit/Main/TWikiUsers (t [1748033129] )
...continues on next page ...

```

...continued from previous page ...
http://192.168.29.195/twiki/bin/edit/Main/TWikiWeb (topicparent [Main.WebHome])
http://192.168.29.195/twiki/bin/edit/Main/TestArea (topicparent [Main.WebHome])
http://192.168.29.195/twiki/bin/edit/Main/TextFormattingFAQ (topicparent [Main.W ↪ebHome])
http://192.168.29.195/twiki/bin/edit/Main/TextFormattingRules (topicparent [Main ↪.WebHome])
http://192.168.29.195/twiki/bin/edit/Main/WebChanges (t [1748033132])
http://192.168.29.195/twiki/bin/edit/Main/WebHome (t [1748033119])
http://192.168.29.195/twiki/bin/edit/Main/WebIndex (t [1748033136])
http://192.168.29.195/twiki/bin/edit/Main/WebNotify (t [1748033158])
http://192.168.29.195/twiki/bin/edit/Main/WebPreferences (t [1748033138])
http://192.168.29.195/twiki/bin/edit/Main/WebSearch (t [1748033136])
http://192.168.29.195/twiki/bin/edit/Main/WebStatistics (t [1748033158])
http://192.168.29.195/twiki/bin/edit/Main/WebTopicEditTemplate (topicparent [Mai ↪n.WebPreferences])
http://192.168.29.195/twiki/bin/edit/Main/WebTopicList (t [1748033157])
http://192.168.29.195/twiki/bin/edit/Main/WelcomeGuest (topicparent [Main.WebHom ↪e])
http://192.168.29.195/twiki/bin/edit/Main/WikiName (topicparent [Main.TWikiUsers ↪])
http://192.168.29.195/twiki/bin/edit/Main/WikiNotation (topicparent [Main.TWikiU ↪sers])
http://192.168.29.195/twiki/bin/edit/Sandbox/TestTopic1 (topicparent [Sandbox.We ↪bHome])
http://192.168.29.195/twiki/bin/edit/Sandbox/TestTopic2 (topicparent [Sandbox.We ↪bHome])
http://192.168.29.195/twiki/bin/edit/Sandbox/TestTopic3 (topicparent [Sandbox.We ↪bHome])
http://192.168.29.195/twiki/bin/edit/Sandbox/TestTopic4 (topicparent [Sandbox.We ↪bHome])
http://192.168.29.195/twiki/bin/edit/Sandbox/TestTopic5 (topicparent [Sandbox.We ↪bHome])
http://192.168.29.195/twiki/bin/edit/Sandbox/TestTopic6 (topicparent [Sandbox.We ↪bHome])
http://192.168.29.195/twiki/bin/edit/Sandbox/TestTopic7 (topicparent [Sandbox.We ↪bHome])
http://192.168.29.195/twiki/bin/edit/Sandbox/TestTopic8 (topicparent [Sandbox.We ↪bHome])
http://192.168.29.195/twiki/bin/edit/Sandbox/WebChanges (t [1748033154])
http://192.168.29.195/twiki/bin/edit/Sandbox/WebHome (t [1748033127])
http://192.168.29.195/twiki/bin/edit/Sandbox/WebIndex (t [1748033250])
http://192.168.29.195/twiki/bin/edit/Sandbox/WebNotify (t [1748033254])
http://192.168.29.195/twiki/bin/edit/Sandbox/WebPreferences (t [1748033156])
http://192.168.29.195/twiki/bin/edit/Sandbox/WebSearch (t [1748033156])
http://192.168.29.195/twiki/bin/edit/Sandbox/WebStatistics (t [1748033254])
http://192.168.29.195/twiki/bin/edit/Sandbox/WebTopicEditTemplate (topicparent [↪Sandbox.WebPreferences])
... continues on next page ...

<p>...continued from previous page...</p> <pre> http://192.168.29.195/twiki/bin/edit/Sandbox/WebTopicList (t [1748033253]) http://192.168.29.195/twiki/bin/edit/TWiki/ (topic [] topicparent [TWikiFAQ] onl ↪ywikiname [on] templatetopic [TWikiFaqTemplate]) http://192.168.29.195/twiki/bin/edit/TWiki/AppendixFileSystem (t [1748033237]) http://192.168.29.195/twiki/bin/edit/TWiki/BumpyWord (t [1748033262]) http://192.168.29.195/twiki/bin/edit/TWiki/DefaultPlugin (t [1748033207]) http://192.168.29.195/twiki/bin/edit/TWiki/FileAttachment (t [1748033204]) http://192.168.29.195/twiki/bin/edit/TWiki/FormattedSearch (t [1748033225]) http://192.168.29.195/twiki/bin/edit/TWiki/GnuGeneralPublicLicense (t [174803324 ↪2]) http://192.168.29.195/twiki/bin/edit/TWiki/GoodStyle (t [1748033183]) http://192.168.29.195/twiki/bin/edit/TWiki/InstalledPlugins (t [1748033240]) http://192.168.29.195/twiki/bin/edit/TWiki/InstantEnhancements (t [1748033211]) http://192.168.29.195/twiki/bin/edit/TWiki/InterWikis (t [1748033209]) http://192.168.29.195/twiki/bin/edit/TWiki/InterwikiPlugin (t [1748033208]) http://192.168.29.195/twiki/bin/edit/TWiki/ManagingTopics (t [1748033234]) http://192.168.29.195/twiki/bin/edit/TWiki/ManagingWebs (t [1748033236]) http://192.168.29.195/twiki/bin/edit/TWiki/MeaningfulTitle (topicparent [TWiki.T ↪extFormattingFAQ]) http://192.168.29.195/twiki/bin/edit/TWiki/NewTopic(topicparent [TWiki.TWikiSho ↪rthand]) http://192.168.29.195/twiki/bin/edit/TWiki/NotExistingYet (topicparent [TWiki.Te ↪xtFormattingRules]) http://192.168.29.195/twiki/bin/edit/TWiki/PeterThoeny (t [1748033241]) http://192.168.29.195/twiki/bin/edit/TWiki/SiteMap (t [1748033240]) http://192.168.29.195/twiki/bin/edit/TWiki/StartingPoints (t [1748033140]) http://192.168.29.195/twiki/bin/edit/TWiki/TWikiAccessControl (t [1748033220]) http://192.168.29.195/twiki/bin/edit/TWiki/TWikiAdminCookBook (t [1748033210]) http://192.168.29.195/twiki/bin/edit/TWiki/TWikiCourseOutlineExample (topicparen ↪t [TWiki.WebHome]) http://192.168.29.195/twiki/bin/edit/TWiki/TWikiFAQ (t [1748033161]) </pre>
<p>Solution:</p>
<p>Log Method Details: Web Application Scanning Consolidation / Info Reporting OID:1.3.6.1.4.1.25623.1.0.111038 Version used: 2025-05-13T05:41:39Z</p>
<p>References url: https://forum.greenbone.net/c/vulnerability-tests/7</p>

Log (CVSS: 0.0)
NVT: PHP Detection (HTTP)
Summary HTTP based detection of PHP.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected PHP Version: 5.2.4 Location: 80/tcp CPE: cpe:/a:php:php:5.2.4 Concluded from version/product identification result: X-Powered-By: PHP/5.2.4-2ubuntu5.10
Solution:
Log Method Details: PHP Detection (HTTP) OID:1.3.6.1.4.1.25623.1.0.800109 Version used: 2025-04-30T05:39:51Z

[\[return to 192.168.29.195 \]](#)

2.1.40 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection
Summary This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A SMB server is running on this port
Solution:
...
... continues on next page ...

...continued from previous page ...
Log Method Details: SMB/CIFS Server Detection OID:1.3.6.1.4.1.25623.1.0.11011 Version used: 2023-08-01T13:29:10Z

[\[return to 192.168.29.195 \]](#)

2.1.41 Log 8787/tcp

Log (CVSS: 0.0) NVT: Service Detection with 'GET' Request
Summary This plugin performs service detection.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A Distributed Ruby (dRuby/DRb) service seems to be running on this port.
Solution:
Vulnerability Insight This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a HTTP 'GET' request to the remaining unknown services and tries to identify them.
Log Method Details: Service Detection with 'GET' Request OID:1.3.6.1.4.1.25623.1.0.17975 Version used: 2025-02-06T05:38:57Z

[\[return to 192.168.29.195 \]](#)

2.1.42 Log 3306/tcp

Log (CVSS: 0.0) NVT: MariaDB / Oracle MySQL Detection (MySQL Protocol)
Summary MySQL protocol-based detection of MariaDB / Oracle MySQL.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected Oracle MySQL Version: 5.0.51a-3ubuntu5 Location: 3306/tcp CPE: cpe:/a:oracle:mysql:5.0.51a Concluded from version/product identification result: 5.0.51a-3ubuntu5
Solution:
Log Method Details: MariaDB / Oracle MySQL Detection (MySQL Protocol) OID:1.3.6.1.4.1.25623.1.0.100152 Version used: 2024-07-19T15:39:06Z

Log (CVSS: 0.0)
NVT: Services
Summary This plugin performs service detection.
Quality of Detection (QoD): 80%
Vulnerability Detection Result An unknown service is running on this port. It is usually reserved for MySQL
Solution:
Vulnerability Insight This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2025-03-05T05:38:53Z

Log (CVSS: 0.0)
NVT: Database Open Access Information Disclosure Vulnerability
Summary Various Database server might be prone to an information disclosure vulnerability if accessible to remote systems.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Oracle MySQL can be accessed by remote attackers
Impact Successful exploitation could allow an attacker to obtain sensitive information from the database.
Solution: Solution type: Workaround Restrict database access to remote systems. Please see the manual of the affected database server for more information.
Affected Software/OS - Oracle MySQL - MariaDB - IBM DB2 - PostgreSQL - IBM solidDB - Oracle Database - Microsoft SQL Server
Vulnerability Insight The remote database server is not restricting direct access from remote systems.
Log Method Checks the result of various database server detections and evaluates their results. Details: Database Open Access Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.902799 Version used: 2024-07-19T15:39:06Z
References url: https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_ds_v1-2.pdf

[[return to 192.168.29.195](#)]

2.1.43 Log 23/tcp

Log (CVSS: 0.0)
NVT: Services
Summary This plugin performs service detection.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A telnet server seems to be running on this port
Solution:
Vulnerability Insight This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2025-03-05T05:38:53Z

Log (CVSS: 0.0)
NVT: Telnet Banner Reporting
<p>Summary</p> <p>This scripts reports the received banner of a Telnet service.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>Remote Telnet banner:</p> <pre> _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ , ' _ ' \ / _ \ _ _ / _ ' / _ _ , \ / _ \ _ _ / _ ' , \ / _ \ _) _ _ / (_ \ _ _ \ _) (_) (_ _) _ _ // _ _ / _ _ _ \ _ _ \ _ _ \ _ _ , _ _ _ _ / . _ _ / _ \ _ _ _ / _ \ _ _ \ _ _ , _ . _ _ / _ \ _ _ _ _ _ _ _ _ Warning: Never expose this VM to an untrusted network! Contact: msfdev[at]metasploit.com Login with msfadmin/msfadmin to get started metasploitable login: ... continues on next page ... </pre>

...continued from previous page ...
Solution:
Log Method Details: Telnet Banner Reporting OID:1.3.6.1.4.1.25623.1.0.10281 Version used: 2025-05-21T05:40:19Z

Log (CVSS: 0.0) NVT: Telnet Service Detection
Summary This scripts tries to detect a Telnet service running at the remote host.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A Telnet server seems to be running on this port
Solution:
Log Method Details: Telnet Service Detection OID:1.3.6.1.4.1.25623.1.0.100074 Version used: 2023-07-28T16:09:08Z
References url: https://tools.ietf.org/html/rfc854

[[return to 192.168.29.195](#)]

2.1.44 Log 111/tcp

Log (CVSS: 0.0) NVT: RPC Portmapper Service Detection (TCP)
Summary TCP based detection of a RPC portmapper service.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected RPC Portmapper Location: 111/tcp CPE: cpe:/a:portmap:portmap Extra information: Possible known aliases / names for this product are 'port mapper', 'rpc.portmap' ↔, 'portmap' or 'rpcbind'
Solution:
Vulnerability Insight The RPC portmapper service is an unsecured protocol for Internet facing systems and should only be used on a trusted network segment, otherwise disabled. The software should be patched and configured properly.
Log Method Details: RPC Portmapper Service Detection (TCP) OID:1.3.6.1.4.1.25623.1.0.108090 Version used: 2023-09-12T05:05:19Z
References cve: CVE-1999-0632 url: https://en.wikipedia.org/wiki/Portmap url: https://datatracker.ietf.org/doc/html/rfc1833

Log (CVSS: 0.0)
NVT: Obtain list of all port mapper registered programs via RPC
Summary This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.
Quality of Detection (QoD): 80%
Vulnerability Detection Result These are the registered RPC programs: RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/ ↔TCP RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/TCP RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/TCP RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/TCP RPC program #100024 version 1 'status' on port 39814/TCP RPC program #100021 version 1 'nlockmgr' on port 44048/TCP
... continues on next page ...

...continued from previous page ...
RPC program #100021 version 3 'nlockmgr' on port 44048/TCP
RPC program #100021 version 4 'nlockmgr' on port 44048/TCP
RPC program #100005 version 1 'mountd' (mount showmount) on port 57550/TCP
RPC program #100005 version 2 'mountd' (mount showmount) on port 57550/TCP
RPC program #100005 version 3 'mountd' (mount showmount) on port 57550/TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/ ↔UDP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/UDP
RPC program #100021 version 1 'nlockmgr' on port 34418/UDP
RPC program #100021 version 3 'nlockmgr' on port 34418/UDP
RPC program #100021 version 4 'nlockmgr' on port 34418/UDP
RPC program #100005 version 1 'mountd' (mount showmount) on port 45740/UDP
RPC program #100005 version 2 'mountd' (mount showmount) on port 45740/UDP
RPC program #100005 version 3 'mountd' (mount showmount) on port 45740/UDP
RPC program #100024 version 1 'status' on port 48481/UDP
Solution:
Log Method Details: Obtain list of all port mapper registered programs via RPC OID:1.3.6.1.4.1.25623.1.0.11111 Version used: 2023-09-08T05:06:21Z

[\[return to 192.168.29.195 \]](#)

2.1.45 Log 1099/tcp

Log (CVSS: 0.0)
NVT: RMI Registry Service Detection
Summary Detection of a Remote Method Invocation (RMI) registry service.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A RMI registry service is running at this port.
Solution:
...
... continues on next page ...

...continued from previous page ...
Log Method Details: RMI Registry Service Detection OID:1.3.6.1.4.1.25623.1.0.105839 Version used: 2025-04-25T15:41:53Z

[\[return to 192.168.29.195 \]](#)

2.1.46 Log 2121/tcp

Log (CVSS: 0.0) NVT: FTP Banner Detection
Summary This script detects and reports a FTP Server Banner.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Remote FTP server banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.29.195] This is probably (a): - ProFTPD Server operating system information collected via "SYST" command: 215 UNIX Type: L8
Solution:
Log Method Details: FTP Banner Detection OID:1.3.6.1.4.1.25623.1.0.10092 Version used: 2025-04-16T05:39:43Z

Log (CVSS: 0.0) NVT: SSL/TLS: FTP Missing Support For AUTH TLS
Summary The remote FTP server does not support the 'AUTH TLS' command.
Quality of Detection (QoD): 80%
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Result

The remote FTP server does not support the 'AUTH TLS' command.

Solution:**Log Method**

Details: SSL/TLS: FTP Missing Support For AUTH TLS

OID:1.3.6.1.4.1.25623.1.0.108553

Version used: 2021-03-19T08:13:38Z

Log (CVSS: 0.0)

NVT: Services

Summary

This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

An FTP server is running on this port.

Here is its banner :

220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.29.195]

Solution:**Vulnerability Insight**

This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method

Details: Services

OID:1.3.6.1.4.1.25623.1.0.10330

Version used: 2025-03-05T05:38:53Z

Log (CVSS: 0.0)

NVT: ProFTPD Server Detection (FTP)

Summary

FTP based detection of the ProFTPD Server.

... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 80%
Vulnerability Detection Result Detected ProFTPD Version: 1.3.1 Location: 2121/tcp CPE: cpe:/a:proftpd:proftpd:1.3.1 Concluded from version/product identification result: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.29.195]
Solution:
Log Method Details: ProFTPD Server Detection (FTP) OID:1.3.6.1.4.1.25623.1.0.900815 Version used: 2025-03-19T05:38:35Z
References url: http://www.proftpd.org

[\[return to 192.168.29.195 \]](#)

2.1.47 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan. Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.
Quality of Detection (QoD): 80%
Vulnerability Detection Result 192.168.29.195 cpe:/a:apache:http_server:2.2.8 192.168.29.195 cpe:/a:beasts:vsftpd:2.3.4 192.168.29.195 cpe:/a:ietf:secure_shell_protocol:2.0 192.168.29.195 cpe:/a:ietf:secure_sockets_layer:2.0
... continues on next page ...

...continued from previous page...	
192.168.29.195	cpe:/a:ietf:secure_sockets_layer:3.0
192.168.29.195	cpe:/a:ietf:transport_layer_security:1.0
192.168.29.195	cpe:/a:isc:bind:9.4.2
192.168.29.195	cpe:/a:jquery:jquery:1.3.2
192.168.29.195	cpe:/a:mysql:mysql:5.0.51a
192.168.29.195	cpe:/a:openbsd:openssh:4.7p1
192.168.29.195	cpe:/a:oracle:mysql:5.0.51a
192.168.29.195	cpe:/a:php:php:5.2.4
192.168.29.195	cpe:/a:phpmyadmin:phpmyadmin:3.1.1
192.168.29.195	cpe:/a:portmap:portmap
192.168.29.195	cpe:/a:postfix:postfix
192.168.29.195	cpe:/a:postgresql:postgresql:8.3.1
192.168.29.195	cpe:/a:proftpd:proftpd:1.3.1
192.168.29.195	cpe:/a:samba:samba:3.0.20
192.168.29.195	cpe:/a:twiki:twiki:01.Feb.2003
192.168.29.195	cpe:/a:unrealircd:unrealircd:3.2.8.1
192.168.29.195	cpe:/o:canonical:ubuntu_linux:8.04
Solution:	
Log Method Details: CPE Inventory OID:1.3.6.1.4.1.25623.1.0.810002 Version used: 2022-07-27T10:11:28Z	
References url: https://nvd.nist.gov/products/cpe	

[\[return to 192.168.29.195 \]](#)

2.1.48 Log 53/tcp

Log (CVSS: 0.0)
NVT: DNS Server Detection (TCP)
Summary TCP based detection of a DNS server.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The remote DNS server banner is: 9.4.2
... continues on next page ...

...continued from previous page ...

Solution:**Log Method**

Details: DNS Server Detection (TCP)

OID:1.3.6.1.4.1.25623.1.0.108018

Version used: 2021-11-30T08:05:58Z

[\[return to 192.168.29.195 \]](#)

2.1.49 Log 513/tcp

Log (CVSS: 0.0)

NVT: Service Detection with 'BINARY' Request

Summary

This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

A rlogin service seems to be running on this port.

Solution:**Vulnerability Insight**

This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a 'BINARY' request to the remaining unknown services and tries to identify them.

Log Method

Details: Service Detection with 'BINARY' Request

OID:1.3.6.1.4.1.25623.1.0.108204

Version used: 2025-03-05T05:38:53Z

[\[return to 192.168.29.195 \]](#)

2.1.50 Log 512/tcp

Log (CVSS: 0.0)
NVT: Service Detection with 'BINARY' Request
Summary This plugin performs service detection.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A rexec service seems to be running on this port.
Solution:
Vulnerability Insight This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a 'BINARY' request to the remaining unknown services and tries to identify them.
Log Method Details: Service Detection with 'BINARY' Request OID:1.3.6.1.4.1.25623.1.0.108204 Version used: 2025-03-05T05:38:53Z

Log (CVSS: 0.0)
NVT: rexec Detection
Summary This remote host is running a rexec service.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The rexec service is not allowing connections from this host.
Solution:
Log Method Details: rexec Detection OID:1.3.6.1.4.1.25623.1.0.113763 Version used: 2023-07-28T16:09:07Z

[[return to 192.168.29.195](#)]

2.1.51 Log 5432/tcp

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection
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 SSL/TLS certificate on this port is self-signed.
Quality of Detection (QoD): 98%
Vulnerability Detection Result The certificate of the remote service is self signed. Certificate details: fingerprint (SHA-1) ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256) E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A ↪F1E32DEE436DE813CC issued by 1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX public key algorithm RSA public key size (bits) 1024 serial 00FAF93A4C7FB6B9CC signature algorithm sha1WithRSAEncryption subject 1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX subject alternative names (SAN) None valid from 2010-03-17 14:07:45 UTC valid until 2010-04-16 14:07:45 UTC
Solution:
Log Method Details: SSL/TLS: Certificate - Self-Signed Certificate Detection OID:1.3.6.1.4.1.25623.1.0.103140 Version used: 2024-06-14T05:05:48Z
... continues on next page ...

...continued from previous page ...
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)
References url: http://en.wikipedia.org/wiki/Self-signed_certificate

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) 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.↵802067)
Summary This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).
Quality of Detection (QoD): 98%
Vulnerability Detection Result Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv ↵ice via the SSLv3 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv ↵ice via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Solution:
Log Method Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites OID:1.3.6.1.4.1.25623.1.0.105018 Version used: 2024-09-30T08:38:05Z
Product Detection Result ... continues on next page ...

...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)

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details
<div><div>Summary</div><div>This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.</div></div>
Quality of Detection (QoD): 98%
<div><div>Vulnerability Detection Result</div><div>The following certificate details of the remote service were collected. 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 ↪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</div></div>
Solution:
<div><div>Log Method</div><div>Details: SSL/TLS: Collect and Report Certificate Details OID:1.3.6.1.4.1.25623.1.0.103692 Version used: 2024-09-27T05:05:23Z</div></div>

Log (CVSS: 0.0)
NVT: PostgreSQL Detection (TCP)
Summary TCP based detection of PostgreSQL.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A PostgreSQL service has been identified on this port.
Solution:
Log Method The script sends a connection request to the server (user:postgres, DB:postgres) and attempts to extract the version number from the reply. Details: PostgreSQL Detection (TCP) OID:1.3.6.1.4.1.25623.1.0.100151 Version used: 2024-07-22T05:05:40Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non 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.↪802067)
Summary This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.
Quality of Detection (QoD): 98%
Vulnerability Detection Result 'Weak' cipher suites accepted by this service via the SSLv3 protocol: TLS_RSA_WITH_RC4_128_SHA 'Non Weak' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA ... continues on next page ...

...continued from previous page ...
TLS_RSA_WITH_AES_256_CBC_SHA 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_SHA 'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
Solution:
Log Method Details: SSL/TLS: Report Non Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103441 Version used: 2024-09-27T05:05:23Z
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)

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites
Summary This routine reports all SSL/TLS cipher suites accepted by a service.
Quality of Detection (QoD): 98%
Vulnerability Detection Result 'Strong' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_WITH_AES_256_CBC_SHA 'Medium' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 'Weak' cipher suites accepted by this service via the SSLv3 protocol: TLS_RSA_WITH_RC4_128_SHA No 'Null' cipher suites accepted by this service via the SSLv3 protocol. No 'Anonymous' cipher suites accepted by this service via the SSLv3 protocol. ... continues on next page ...

...continued from previous page ...
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_AES_256_CBC_SHA 'Medium' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_SHA No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
Solution:
Vulnerability Insight Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.
Log Method Details: SSL/TLS: Report Supported Cipher Suites OID:1.3.6.1.4.1.25623.1.0.802067 Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Untrusted Certificate Detection
Summary Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.
Quality of Detection (QoD): 98%
Vulnerability Detection Result The remote SSL/TLS server is using the following certificate(s) which failed the ↪ verification against the system wide trust store (serial:issuer): 00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652 ↪E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complicati ↪on of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing ... continues on next page ...

...continued from previous page ...
↔outside US,C=XX (Server certificate)
Solution:
Log Method Details: SSL/TLS: Untrusted Certificate Detection OID:1.3.6.1.4.1.25623.1.0.117764 Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Safe/Secure Renegotiation Support Status
Summary Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.
Quality of Detection (QoD): 98%
Vulnerability Detection Result Protocol Version Safe/Secure Renegotiation Support Status ----- ↔----- ↔----- SSLv3 Unknown, Reason: Scanner failed to negotiate an SSL/TLS connection (Either the scanner or the remote host is probably not supporting / accepting this SSL/TLS protocol version). TLSv1.0 Enabled, Note: While the remote service announces the support of safe/secure renegotiation it still might not support / accept renegotiation at all. TLSv1.1 Unknown, Reason: Scanner failed to negotiate an SSL/TLS connection (Either the scanner or the remote host is probably not supporting / accepting this SSL/TLS protocol version). TLSv1.2 Unknown, Reason: Scanner failed to negotiate an SSL/TLS connection (Either the scanner or the remote host is probably not supporting / accepting this SSL/TLS protocol version). TLSv1.3 Unknown, Reason: Scanner failed to negotiate an SSL/TLS connection (Either the scanner or the remote host is probably not supporting / accepting this SSL/TLS protocol version).
Solution:
Log Method Details: SSL/TLS: Safe/Secure Renegotiation Support Status OID:1.3.6.1.4.1.25623.1.0.117757
... continues on next page ...

...continued from previous page ...
Version used: 2024-09-27T05:05:23Z
References url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)
NVT: Services
Summary This plugin performs service detection.
Quality of Detection (QoD): 80%
Vulnerability Detection Result An unknown service is running on this port. It is usually reserved for Postgres
Solution:
Vulnerability Insight This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2025-03-05T05:38:53Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium 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.↔802067)
Summary ... continues on next page ...

...continued from previous page ...
This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Quality of Detection (QoD): 98%
Vulnerability Detection Result 'Medium' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 'Medium' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
Solution:
Vulnerability Insight Any cipher suite considered to be secure for only the next 10 years is considered as medium.
Log Method Details: SSL/TLS: Report Medium Cipher Suites OID:1.3.6.1.4.1.25623.1.0.902816 Version used: 2024-09-27T05:05:23Z
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)

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection
Summary Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The remote SSL/TLS service supports the following SSL/TLS protocol version(s): SSLv3
... continues on next page ...

...continued from previous page ...
TLSv1.0
Solution:
Log Method Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies. Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers. Details: SSL/TLS: Version Detection OID:1.3.6.1.4.1.25623.1.0.105782 Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: PostgreSQL SSL/TLS Support Detection (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 Checks if the remote PostgreSQL server supports SSL/TLS.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The remote PostgreSQL server supports SSL/TLS.
Solution:
Log Method Details: SSL/TLS: PostgreSQL SSL/TLS Support Detection (PostgreSQL Protocol) OID:1.3.6.1.4.1.25623.1.0.105013 Version used: 2024-07-24T05:06:37Z
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)
... continues on next page ...

...continued from previous page ...

Referencesurl: <https://www.postgresql.org/docs/current/static/ssl-tcp.html>[\[return to 192.168.29.195 \]](#)**2.1.52 Log 6697/tcp**

Log (CVSS: 0.0)

NVT: Service Detection with 'GET' Request

Summary

This plugin performs service detection.

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

An IRC server seems to be running on this port.

Solution:**Vulnerability Insight**

This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a HTTP 'GET' request to the remaining unknown services and tries to identify them.

Log Method

Details: Service Detection with 'GET' Request

OID:1.3.6.1.4.1.25623.1.0.17975

Version used: 2025-02-06T05:38:57Z

Log (CVSS: 0.0)

NVT: UnrealIRCd Detection

Summary

Detection of UnrealIRCd Daemon. This script sends a request to the server and gets the version from the response.

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

Detected UnrealIRCd

... continues on next page ...

...continued from previous page ...	
Version:	3.2.8.1
Location:	6697/tcp
CPE:	cpe:/a:unrealircd:unrealircd:3.2.8.1
Concluded from version/product identification result: Unreal3.2.8.1	
Solution:	
Log Method Details: UnrealIRCd Detection OID:1.3.6.1.4.1.25623.1.0.809884 Version used: 2022-06-01T21:00:42Z	

Log (CVSS: 0.0)	
NVT: IRC Server Banner Detection	
Summary This script tries to detect the banner of an IRC server.	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result The IRC server banner is: :irc.Metasploitable.LAN 351 HIGGEGJEA Unreal3.2.8.1. irc.Metasploitable.LAN :Fhi ↪X0oE [*=2309]	
Solution:	
Log Method Details: IRC Server Banner Detection OID:1.3.6.1.4.1.25623.1.0.11156 Version used: 2023-08-01T13:29:10Z	

[\[return to 192.168.29.195 \]](#)

2.1.53 Log 445/tcp

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection
Summary Detection of Server Message Block(SMB). This script sends SMB Negotiation request and try to get the version from the response.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Only SMBv1 is enabled on remote target
Solution:
Log Method Details: SMB Remote Version Detection OID:1.3.6.1.4.1.25623.1.0.807830 Version used: 2023-07-26T05:05:09Z

Log (CVSS: 0.0)
NVT: Microsoft SMB Signing Disabled
Summary Checks if SMB Signing is disabled at the remote SMB server.
Quality of Detection (QoD): 80%
Vulnerability Detection Result SMB Signing is disabled at the server.
Solution:
Log Method Details: Microsoft SMB Signing Disabled OID:1.3.6.1.4.1.25623.1.0.802726 Version used: 2023-07-25T05:05:58Z

Log (CVSS: 0.0)
NVT: SMB Login Successful For Authenticated Checks
Summary It was possible to login using the provided SMB credentials. Hence authenticated checks are enabled.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution:
Log Method Details: SMB Login Successful For Authenticated Checks OID:1.3.6.1.4.1.25623.1.0.108539 Version used: 2023-07-28T16:09:07Z

Log (CVSS: 0.0)
NVT: SMBv1 Enabled - Active Check
Summary The host has enabled SMBv1 for the SMB Server.
Quality of Detection (QoD): 80%
Vulnerability Detection Result SMBv1 is enabled for the SMB Server
Solution:
Log Method Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT: - SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830). Details: SMBv1 Enabled - Active Check OID:1.3.6.1.4.1.25623.1.0.140151 Version used: 2024-01-09T05:06:46Z
References url: https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best- ... continues on next page ...

...continued from previous page...

↔Practices

url: <https://support.microsoft.com/en-us/kb/2696547>url: <https://support.microsoft.com/en-us/kb/204279>

Log (CVSS: 0.0)

NVT: Microsoft Windows SMB Accessible Shares

Summary

The script detects the Windows SMB Accessible Shares and sets the result into KB.

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

The following shares were found

IPC\$

Solution:**Log Method**

Details: Microsoft Windows SMB Accessible Shares

OID:1.3.6.1.4.1.25623.1.0.902425

Version used: 2025-04-16T05:39:43Z

Log (CVSS: 0.0)

NVT: SMB log in

Summary

This script attempts to logon into the remote host using login/password credentials.

Quality of Detection (QoD): 97%**Vulnerability Detection Result**

It was possible to log into the remote host using the SMB protocol.

Solution:**Log Method**

Details: SMB log in

OID:1.3.6.1.4.1.25623.1.0.10394

Version used: 2025-04-16T05:39:43Z

Log (CVSS: 0.0)
NVT: SMB NativeLanMan
Summary It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.
Quality of Detection (QoD): 95%
Vulnerability Detection Result Detected SMB workgroup: WORKGROUP Detected SMB server: Samba 3.0.20-Debian Detected OS: Debian GNU/Linux
Solution:
Log Method Details: SMB NativeLanMan OID:1.3.6.1.4.1.25623.1.0.102011 Version used: 2024-06-25T05:05:27Z

Log (CVSS: 0.0)
NVT: SMB NativeLanMan
Summary It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.
Quality of Detection (QoD): 95%
Vulnerability Detection Result Detected Samba Version: 3.0.20 Location: 445/tcp CPE: cpe:/a:samba:samba:3.0.20 Concluded from version/product identification result: Samba 3.0.20-Debian Extra information: Detected SMB workgroup: WORKGROUP Detected SMB server: Samba 3.0.20-Debian
Solution:
... continues on next page ...

...continued from previous page ...
Log Method Details: SMB NativeLanMan OID:1.3.6.1.4.1.25623.1.0.102011 Version used: 2024-06-25T05:05:27Z

Log (CVSS: 0.0) NVT: SMB/CIFS Server Detection
Summary This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A CIFS server is running on this port
Solution:
Log Method Details: SMB/CIFS Server Detection OID:1.3.6.1.4.1.25623.1.0.11011 Version used: 2023-08-01T13:29:10Z

[\[return to 192.168.29.195 \]](#)

2.1.54 Log 1524/tcp

Log (CVSS: 0.0) NVT: Service Detection with 'GET' Request
Summary This plugin performs service detection.
Quality of Detection (QoD): 80%
Vulnerability Detection Result A root shell of Metasploitable seems to be running on this port.
... continues on next page ...

...continued from previous page ...

Solution:**Vulnerability Insight**

This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a HTTP 'GET' request to the remaining unknown services and tries to identify them.

Log Method

Details: Service Detection with 'GET' Request

OID:1.3.6.1.4.1.25623.1.0.17975

Version used: 2025-02-06T05:38:57Z

[\[return to 192.168.29.195 \]](#)

2.1.55 Log 22/tcp

Log (CVSS: 0.0)

NVT: Services

Summary

This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

An ssh server is running on this port

Solution:**Vulnerability Insight**

This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method

Details: Services

OID:1.3.6.1.4.1.25623.1.0.10330

Version used: 2025-03-05T05:38:53Z

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported
<div><div>Summary</div><div>Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.</div></div>
Quality of Detection (QoD): 95%
<div><div>Vulnerability Detection Result</div><div>The remote SSH Server supports the following SSH Protocol Versions: 1.99 2.0</div></div>
Solution:
<div><div>Log Method</div><div>The following versions are tried: 1.33, 1.5, 1.99 and 2.0. Details: SSH Protocol Versions Supported OID:1.3.6.1.4.1.25623.1.0.100259 Version used: 2024-06-17T08:31:37Z</div></div>

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported
<div><div>Summary</div><div>This script detects which algorithms are supported by the remote SSH service.</div></div>
Quality of Detection (QoD): 80%
<div><div>Vulnerability Detection Result</div><div>The following options are supported by the remote SSH service: kex_algorithms: diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-h ↪ellman-group14-sha1,diffie-hellman-group1-sha1 server_host_key_algorithms: ssh-rsa,ssh-dss encryption_algorithms_client_to_server: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19 ↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr encryption_algorithms_server_to_client: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19 ↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr ... continues on next page ...</div></div>

...continued from previous page ...
mac_algorithms_client_to_server: hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com ↔,hmac-sha1-96,hmac-md5-96 mac_algorithms_server_to_client: hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com ↔,hmac-sha1-96,hmac-md5-96 compression_algorithms_client_to_server: none,zlib@openssh.com compression_algorithms_server_to_client: none,zlib@openssh.com
Solution:
Log Method Details: SSH Protocol Algorithms Supported OID:1.3.6.1.4.1.25623.1.0.105565 Version used: 2024-06-17T08:31:37Z

Log (CVSS: 0.0)
NVT: SSH Server type and version
Summary This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Remote SSH server banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 Remote SSH supported authentication: none,password,publickey,hostbased,keyboard-↔interactive Remote SSH text/login banner: (not available) This is probably (a): - OpenSSH Concluded from remote connection attempt with credentials: Login: OpenVASVT Password: OpenVASVT
Solution:
Vulnerability Insight ... continues on next page ...

...continued from previous page ...

This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Log Method

Details: SSH Server type and version

OID:1.3.6.1.4.1.25623.1.0.10267

Version used: 2025-04-25T05:39:37Z

[\[return to 192.168.29.195 \]](#)

This file was automatically generated.