

# Scan Report

August 20, 2023

## Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP 192.168.50.239”. The scan started at Sun Aug 20 17:24:50 2023 UTC and ended at Sun Aug 20 17:56:48 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

<b>1</b>	<b>Result Overview</b>	<b>2</b>
1.1	Host Authentications . . . . .	2
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	192.168.50.239 . . . . .	2
2.1.1	High 5432/tcp . . . . .	3
2.1.2	High 6200/tcp . . . . .	6
2.1.3	High 3632/tcp . . . . .	6
2.1.4	High 1524/tcp . . . . .	7
2.1.5	High 5900/tcp . . . . .	8
2.1.6	High 8009/tcp . . . . .	9
2.1.7	High 8787/tcp . . . . .	15
2.1.8	High 1099/tcp . . . . .	16
2.1.9	High 80/tcp . . . . .	18
2.1.10	High 21/tcp . . . . .	22
2.1.11	High 2121/tcp . . . . .	24
2.1.12	High 3306/tcp . . . . .	25
2.1.13	High 6697/tcp . . . . .	26
2.1.14	High 513/tcp . . . . .	28
2.1.15	High general/tcp . . . . .	29
2.1.16	Medium 23/tcp . . . . .	30
2.1.17	Medium 5432/tcp . . . . .	31

2.1.18	Medium 5900/tcp . . . . .	45
2.1.19	Medium 22/tcp . . . . .	46
2.1.20	Medium 25/tcp . . . . .	49
2.1.21	Medium 80/tcp . . . . .	65
2.1.22	Medium 21/tcp . . . . .	77
2.1.23	Medium 2121/tcp . . . . .	78
2.1.24	Medium 445/tcp . . . . .	79
2.1.25	Low 5432/tcp . . . . .	80
2.1.26	Low general/icmp . . . . .	83
2.1.27	Low 22/tcp . . . . .	84
2.1.28	Low 25/tcp . . . . .	85
2.1.29	Low general/tcp . . . . .	90

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
<a href="#">192.168.50.239</a>	21	39	6	0	0
Total: 1	21	39	6	0	0

Vendor security updates are not trusted.

Overrides are off. Even when a result has an override, this report uses the actual threat of the result.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found.

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

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

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

Only results with a minimum QoD of 70 are shown.

This report contains all 66 results selected by the filtering described above. Before filtering there were 581 results.

### 1.1 Host Authentications

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

## 2 Results per Host

### 2.1 192.168.50.239

Host scan start Sun Aug 20 17:25:25 2023 UTC

Host scan end Sun Aug 20 17:56:39 2023 UTC

Service (Port)	Threat Level
<a href="#">5432/tcp</a>	High
<a href="#">6200/tcp</a>	High
<a href="#">3632/tcp</a>	High
<a href="#">1524/tcp</a>	High
<a href="#">5900/tcp</a>	High
<a href="#">8009/tcp</a>	High
<a href="#">8787/tcp</a>	High
<a href="#">1099/tcp</a>	High
<a href="#">80/tcp</a>	High

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
21/tcp	High
2121/tcp	High
3306/tcp	High
6697/tcp	High
513/tcp	High
general/tcp	High
23/tcp	Medium
5432/tcp	Medium
5900/tcp	Medium
22/tcp	Medium
25/tcp	Medium
80/tcp	Medium
21/tcp	Medium
2121/tcp	Medium
445/tcp	Medium
5432/tcp	Low
general/icmp	Low
22/tcp	Low
25/tcp	Low
general/tcp	Low

**2.1.1 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 (TCP) (OID: 1.3.6.1.4.1.25623.1.0.100151)

**Summary**

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

**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)

... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.103552 Version used: 2023-07-25T05:05:58Z
<b>Product Detection Result</b> Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection (TCP) OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>High (CVSS: 7.4)</b> <b>NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability</b>
<b>Summary</b> OpenSSL is prone to security-bypass vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Send two SSL ChangeCipherSpec request and check the response. Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.105042 Version used: 2023-07-26T05:05:09Z
<b>References</b> cve: CVE-2014-0224 url: <a href="https://www.openssl.org/news/secadv/20140605.txt">https://www.openssl.org/news/secadv/20140605.txt</a> url: <a href="http://www.securityfocus.com/bid/67899">http://www.securityfocus.com/bid/67899</a> cert-bund: WID-SEC-2023-0500
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0567  
 cert-bund: CB-K15/0415  
 cert-bund: CB-K15/0384  
 cert-bund: CB-K15/0080  
 cert-bund: CB-K15/0079  
 cert-bund: CB-K15/0074  
 cert-bund: CB-K14/1617  
 cert-bund: CB-K14/1537  
 cert-bund: CB-K14/1299  
 cert-bund: CB-K14/1297  
 cert-bund: CB-K14/1294  
 cert-bund: CB-K14/1202  
 cert-bund: CB-K14/1174  
 cert-bund: CB-K14/1153  
 cert-bund: CB-K14/0876  
 cert-bund: CB-K14/0756  
 cert-bund: CB-K14/0746  
 cert-bund: CB-K14/0736  
 cert-bund: CB-K14/0722  
 cert-bund: CB-K14/0716  
 cert-bund: CB-K14/0708  
 cert-bund: CB-K14/0684  
 cert-bund: CB-K14/0683  
 cert-bund: CB-K14/0680  
 dfn-cert: DFN-CERT-2016-0388  
 dfn-cert: DFN-CERT-2015-0593  
 dfn-cert: DFN-CERT-2015-0427  
 dfn-cert: DFN-CERT-2015-0396  
 dfn-cert: DFN-CERT-2015-0082  
 dfn-cert: DFN-CERT-2015-0079  
 dfn-cert: DFN-CERT-2015-0078  
 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

...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2014-0709

[\[ return to 192.168.50.239 \]](#)**2.1.2 High 6200/tcp****High (CVSS: 7.5)****NVT: vsftpd Compromised Source Packages Backdoor Vulnerability****Summary**

vsftpd is prone to a backdoor vulnerability.

**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 link. Please validate the package with its signature.

**Affected Software/OS**

The vsftpd 2.3.4 source package is affected.

**Vulnerability Detection Method**

Details: vsftpd Compromised Source Packages Backdoor Vulnerability

OID:1.3.6.1.4.1.25623.1.0.103185

Version used: 2023-07-28T05:05:23Z

**References**url: <http://www.securityfocus.com/bid/48539>url: <http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html>url: <https://security.appspot.com/vsftpd.html>[\[ return to 192.168.50.239 \]](#)**2.1.3 High 3632/tcp**

<p>High (CVSS: 9.3) NVT: DistCC RCE Vulnerability (CVE-2004-2687)</p>
<p><b>Summary</b> DistCC is prone to a remote code execution (RCE) vulnerability.</p>
<p><b>Vulnerability Detection Result</b> It was possible to execute the "id" command. Result: uid=1(daemon) gid=1(daemon)</p>
<p><b>Impact</b> DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.</p>
<p><b>Solution:</b> <b>Solution type:</b> VendorFix Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references.</p>
<p><b>Vulnerability Insight</b> 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><b>Vulnerability Detection Method</b> Details: DistCC RCE Vulnerability (CVE-2004-2687) OID:1.3.6.1.4.1.25623.1.0.103553 Version used: 2022-07-07T10:16:06Z</p>
<p><b>References</b> cve: CVE-2004-2687 url: <a href="https://distcc.github.io/security.html">https://distcc.github.io/security.html</a> url: <a href="https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80/→/archives/bugtraq/2005-03/0183.html">https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80/→/archives/bugtraq/2005-03/0183.html</a> dfn-cert: DFN-CERT-2019-0381</p>

[ [return to 192.168.50.239](#) ]

#### 2.1.4 High 1524/tcp

<p>High (CVSS: 10.0) NVT: Possible Backdoor: Ingreslock</p>
<p><b>Summary</b> A backdoor is installed on the remote host.</p>
<p>... continues on next page ...</p>



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

[ [return to 192.168.50.239](#) ]

### 2.1.5 High 5900/tcp

High (CVSS: 9.0) NVT: VNC Brute Force Login
<b>Summary</b> Try to log in with given passwords via VNC protocol.
<b>Vulnerability Detection Result</b> It was possible to connect to the VNC server with the password: password
<b>Solution:</b> <b>Solution type:</b> Mitigation Change the password to something hard to guess or enable password protection at all.
<b>Vulnerability Insight</b> This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all. Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked. Note as well that passwords can be max. 8 characters long.
... continues on next page ...

...continued from previous page...

**Vulnerability Detection Method**

Details: VNC Brute Force Login

OID:1.3.6.1.4.1.25623.1.0.106056

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

[\[ return to 192.168.50.239 \]](#)**2.1.6 High 8009/tcp**

High (CVSS: 9.8)

NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

**Summary**

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

**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\x001FÃ\x0003\x001FÃ, <!--
```

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

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

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

```
-->
```

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

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

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

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

```
<head>
```

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

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

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

```
body {
```

```
color: #000000;
```

```
background-color: #FFFFFF;
```

```
font-family: Arial, "Times New Roman", Times, serif;
```

...continues on next page...

...continued from previous page ...

```
        margin: 10px 0px;
    }
    img {
        border: none;
    }

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

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

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

...continues on next page ...

...continued from previous page ...

```

/*]]>*/
</style>
</head>
<body>
<!-- Header -->
<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>
        <tr>
          <td class="menu">
            <a href="RELEASE-NOTES.txt">Release&nbsp;Notes</a><br/>

```

...continues on next page ...

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

...continued from previous page...

```

        </tr>
    </table>

    <br/>
    <table width="100%" border="1" cellspacing="0" cellpadding="3">
        <tr>
            <th>Miscellaneous</th>
        </tr>
        <tr>
            <td class="menu">
                <a href="http://java.sun.com/products/jsp">Sun's Java &
                ↪ nbsp;Server & nbsp;Pages & nbsp;Site</a><br/>
                <a href="http://java.sun.com/products/servlet">Sun's 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
    is restricted to users with role "admin". The manager webapp
    is restricted to users with role "manager".</b>
    Users are defined in <code>${CATALINA_HOME}/conf/tomcat-users.xml</cod
    ...continues on next page ...

```

<p style="text-align: right;">...continued from previous page ...</p> <pre> &lt;e&gt;.&lt;/p&gt;     &lt;p&gt;Included with this release are a host of sample Servlets and JSPs     &lt;↳ (with associated source code), extensive documentation (including the Servlet     &lt;↳ 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web app     &lt;↳ lications.&lt;/p&gt;         &lt;p&gt;Tomcat mailing lists are available at the Tomcat project web site     &lt;↳ :&lt;/p&gt;         &lt;ul&gt;             &lt;li&gt;&lt;b&gt;&lt;a href="mailto:users@tomcat.apache.org"&gt;users@tomc </pre>	<p><b>Solution:</b>  <b>Solution type:</b> 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><b>Affected Software/OS</b>  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><b>Vulnerability Insight</b>  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><b>Vulnerability Detection Method</b>  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: 2023-07-06T05:05:36Z</p>	<p><b>References</b>  cve: CVE-2020-1938  cisa: Known Exploited Vulnerability (KEV) catalog  url: <a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">https://www.cisa.gov/known-exploited-vulnerabilities-catalog</a>  url: <a href="https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1">https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1</a>  ↳ a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E  url: <a href="https://www.chaitin.cn/en/ghostcat">https://www.chaitin.cn/en/ghostcat</a>  url: <a href="https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487">https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487</a>  url: <a href="https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi">https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi</a>  url: <a href="https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances">https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances</a>  ↳ -to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/  url: <a href="https://tomcat.apache.org/tomcat-7.0-doc/changelog.html">https://tomcat.apache.org/tomcat-7.0-doc/changelog.html</a>  url: <a href="https://tomcat.apache.org/tomcat-8.5-doc/changelog.html">https://tomcat.apache.org/tomcat-8.5-doc/changelog.html</a>  url: <a href="https://tomcat.apache.org/tomcat-9.0-doc/changelog.html">https://tomcat.apache.org/tomcat-9.0-doc/changelog.html</a>  cert-bund: CB-K20/0711  cert-bund: CB-K20/0705</p>
... continues on next page ...	

...continued from previous page ...

```

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

```

[\[ return to 192.168.50.239 \]](#)

### 2.1.7 High 8787/tcp

**High (CVSS: 10.0)****NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities**

#### Summary

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

#### Vulnerability Detection Result

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:

```

Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'syscall'"0/usr/lib/
↵ruby/1.8/drb/drb.rb:1555:in 'send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in '__se
↵nd__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'perform_without_block'"3/usr/lib/
↵ruby/1.8/drb/drb.rb:1515:in 'perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in 'm
↵ain_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in 'loop'"5/usr/lib/ruby/1.8/drb/
↵drb.rb:1585:in 'main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in 'start'"5/usr
↵/lib/ruby/1.8/drb/drb.rb:1581:in 'main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:143
↵0:in 'run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in 'start'"//usr/lib/ruby/1.8/dr
↵b/drb.rb:1427:in 'run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in 'initialize'"//us
↵r/lib/ruby/1.8/drb/drb.rb:1627:in 'new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
↵'start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
↵plemented

```

#### Impact

... continues on next page ...



...continued from previous page ...
<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><b>Solution:</b>  <b>Solution type:</b> Mitigation  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"> <li>- Implementing taint on untrusted input</li> <li>- Setting \$SAFE levels appropriately (<math>\geq 2</math> is recommended if untrusted hosts are allowed to submit Ruby commands, and <math>\geq 3</math> may be appropriate)</li> <li>- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts</li> </ul>
<p><b>Vulnerability Detection Method</b>  Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.  Details: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities  OID:1.3.6.1.4.1.25623.1.0.108010  Version used: 2023-07-20T05:05:17Z</p>
<p><b>References</b>  url: <a href="https://tools.cisco.com/security/center/viewAlert.x?alertId=22750">https://tools.cisco.com/security/center/viewAlert.x?alertId=22750</a>  url: <a href="http://www.securityfocus.com/bid/47071">http://www.securityfocus.com/bid/47071</a>  url: <a href="http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testing/">http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testing/</a>  url: <a href="http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html">http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html</a></p>

[ [return to 192.168.50.239](#) ]

### 2.1.8 High 1099/tcp

<p>High (CVSS: 7.5)  NVT: Java RMI Server Insecure Default Configuration RCE Vulnerability</p>
<p><b>Summary</b>  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.</p>
<p><b>Vulnerability Detection Result</b>  By doing an RMI request it was possible to trigger the vulnerability and make the remote host sending a request back to the scanner host (Details on the received packet follows).</p>
... continues on next page ...

...continued from previous page...
Destination IP: 192.168.50.130 (receiving IP on scanner host side) Destination port: 10179/tcp (receiving port on scanner host side) Originating IP: 192.168.50.239 (originating IP from target host side)
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> Workaround Disable class-loading. Please contact the vendor of the affected system for additional guidance.
<b>Vulnerability Insight</b> The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software.
<b>Vulnerability Detection Method</b> Sends a crafted JRMII request and checks if the target tries to load a Java class via a remote HTTP URL. 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 OID:1.3.6.1.4.1.25623.1.0.140051 Version used: 2022-12-21T10:12:09Z
<b>References</b> cve: CVE-2011-3556 url: <a href="https://web.archive.org/web/20211208040855/http://www.securitytracker.com/id?1026215">https://web.archive.org/web/20211208040855/http://www.securitytracker.com/id?1026215</a> url: <a href="https://web.archive.org/web/20110824060234/http://download.oracle.com/javase/1.3/docs/guide/rmi/spec/rmi-protocol.html">https://web.archive.org/web/20110824060234/http://download.oracle.com/javase/1.3/docs/guide/rmi/spec/rmi-protocol.html</a> url: <a href="https://tools.cisco.com/security/center/viewAlert.x?alertId=23665">https://tools.cisco.com/security/center/viewAlert.x?alertId=23665</a> 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
...continues on next page...

...continued from previous page ...

```
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
```

[\[ return to 192.168.50.239 \]](#)

### 2.1.9 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.

**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.

... continues on next page ...

...continued from previous page ...
- %SEARCH}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.
<b>Vulnerability Detection Method</b> Details: TWiki XSS and Command Execution Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.800320 Version used: 2023-07-28T05:05:23Z
<b>References</b> cve: CVE-2008-5304 cve: CVE-2008-5305 url: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304 url: http://www.securityfocus.com/bid/32668 url: http://www.securityfocus.com/bid/32669 url: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5305
<b>High (CVSS: 7.5)</b> <b>NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.</b>
<b>Summary</b> PHP is prone to an information-disclosure vulnerability.
<b>Vulnerability Detection Result</b> By doing the following HTTP POST request: "HTTP POST" body : <?php phpinfo();?> URL : http://192.168.50.239/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,NO ↪ARCHIVE" /></head>
<b>Impact</b> Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.
<b>Solution:</b> <b>Solution type:</b> VendorFix PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.
... 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**

Sends a crafted HTTP POST request and checks the response.

Details: PHP-CGI-based setups vulnerability when parsing query string parameters from ph.  
↪..

OID:1.3.6.1.4.1.25623.1.0.103482

Version used: 2022-08-09T10:11:17Z

**References**

cve: CVE-2012-1823

cve: CVE-2012-2311

cve: CVE-2012-2336

cve: CVE-2012-2335

cisa: Known Exploited Vulnerability (KEV) catalog

url: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

url: <http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-ri>  
↪sks-Update-1567532.html

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

url: <http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/>

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

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

url: <http://www.securityfocus.com/bid/53388>

dfn-cert: DFN-CERT-2013-1494

dfn-cert: DFN-CERT-2012-1316

dfn-cert: DFN-CERT-2012-1276

dfn-cert: DFN-CERT-2012-1268

dfn-cert: DFN-CERT-2012-1267

dfn-cert: DFN-CERT-2012-1266

dfn-cert: DFN-CERT-2012-1173

dfn-cert: DFN-CERT-2012-1101

dfn-cert: DFN-CERT-2012-0994

dfn-cert: DFN-CERT-2012-0993

dfn-cert: DFN-CERT-2012-0992

dfn-cert: DFN-CERT-2012-0920

dfn-cert: DFN-CERT-2012-0915

dfn-cert: DFN-CERT-2012-0914

dfn-cert: DFN-CERT-2012-0913

...continues on next page ...

...continued from previous page ...

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: phpinf() output Reporting

### Summary

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

### Vulnerability Detection Result

The following files are calling the function phpinf() which disclose potentiall  
 ↳y sensitive information:

http://192.168.50.239/mutillidae/phpinf.php

http://192.168.50.239/phpinf.php

### Impact

Some of the information that can be gathered from this file includes:

The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

### Solution:

**Solution type:** Workaround

Delete the listed files or restrict access to them.

### Vulnerability Detection Method

Details: phpinf() output Reporting

OID:1.3.6.1.4.1.25623.1.0.11229

Version used: 2023-06-22T10:34:15Z

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.

### Vulnerability Detection Result

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

http://192.168.50.239/dav/puttest1412285277.html

... continues on next page ...

...continued from previous page ...
We could delete the following files via the DELETE method at this web server: <a href="http://192.168.50.239/dav/puttest1412285277.html">http://192.168.50.239/dav/puttest1412285277.html</a>
<b>Impact</b> - 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.
<b>Solution:</b> <b>Solution type:</b> Mitigation Use access restrictions to these dangerous HTTP methods or disable them completely.
<b>Affected Software/OS</b> Web servers with enabled PUT and/or DELETE methods.
<b>Vulnerability Detection Method</b> Checks if dangerous HTTP methods such as PUT and DELETE are enabled and can be misused to upload or delete files. Details: Test HTTP dangerous methods OID:1.3.6.1.4.1.25623.1.0.10498 Version used: 2023-08-01T13:29:10Z
<b>References</b> url: <a href="http://www.securityfocus.com/bid/12141">http://www.securityfocus.com/bid/12141</a> owasp: OWASP-CM-001

[ [return to 192.168.50.239](#) ]

### 2.1.10 High 21/tcp

High (CVSS: 7.5) NVT: vsftpd Compromised Source Packages Backdoor Vulnerability
<b>Summary</b> vsftpd is prone to a backdoor vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
... continues on next page ...

...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> VendorFix The repaired package can be downloaded from the referenced link. Please validate the package with its signature.
<b>Affected Software/OS</b> The vsftpd 2.3.4 source package is affected.
<b>Vulnerability Detection Method</b> Details: vsftpd Compromised Source Packages Backdoor Vulnerability OID:1.3.6.1.4.1.25623.1.0.103185 Version used: 2023-07-28T05:05:23Z
<b>References</b> url: <a href="http://www.securityfocus.com/bid/48539">http://www.securityfocus.com/bid/48539</a> url: <a href="http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html">http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html</a> url: <a href="https://security.appspot.com/vsftpd.html">https://security.appspot.com/vsftpd.html</a>

High (CVSS: 7.5)

NVT: FTP Brute Force Logins Reporting

### Summary

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

### 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.

### 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

... continues on next page ...



...continued from previous page ...
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.
<b>Vulnerability Detection Method</b> Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717). Details: FTP Brute Force Logins Reporting OID:1.3.6.1.4.1.25623.1.0.108718 Version used: 2023-07-06T05:05:36Z
<b>References</b> cve: CVE-1999-0501 cve: CVE-1999-0502 cve: CVE-1999-0507 cve: CVE-1999-0508 cve: CVE-2001-1594 cve: CVE-2013-7404 cve: CVE-2018-19063 cve: CVE-2018-19064

[\[ return to 192.168.50.239 \]](#)

### 2.1.11 High 2121/tcp

High (CVSS: 7.5) NVT: FTP Brute Force Logins Reporting
<b>Summary</b> It was possible to login into the remote FTP server using weak/known credentials.
<b>Vulnerability Detection Result</b> It was possible to login with the following credentials <User>:<Password> msfadmin:msfadmin postgres:postgres service:service user:user
<b>Impact</b> This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.
<b>Solution:</b> <b>Solution type:</b> Mitigation Change the password as soon as possible.
... 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-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices

Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

**Vulnerability Detection Method**

Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).

Details: FTP Brute Force Logins Reporting

OID:1.3.6.1.4.1.25623.1.0.108718

Version used: 2023-07-06T05:05:36Z

**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-2018-19063  
 cve: CVE-2018-19064

[\[ return to 192.168.50.239 \]](#)

**2.1.12 High 3306/tcp**

High (CVSS: 7.8)

NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)

**Product detection result**

cpe:/a:mysql:mysql:5.0.51a

Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.25623.1.0.100152)

**Summary**

It was possible to login into the remote MySQL as root using weak credentials.

**Vulnerability Detection Result**

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

...continues on next page ...

...continued from previous page ...

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

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

**Affected Software/OS**

The following products are known to use such weak credentials:

- CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x
- CVE-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

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: 2023-04-17T10:19:34Z

**Product Detection Result**

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

Method: MariaDB / Oracle MySQL Detection (MySQL Protocol)

OID: 1.3.6.1.4.1.25623.1.0.100152)

**References**

- cve: CVE-2001-0645
- cve: CVE-2004-2357
- cve: CVE-2006-1451
- cve: CVE-2007-2554
- cve: CVE-2007-6081
- cve: CVE-2009-0919
- cve: CVE-2014-3419
- cve: CVE-2015-4669
- cve: CVE-2016-6531
- cve: CVE-2018-15719

[\[ return to 192.168.50.239 \]](#)**2.1.13 High 6697/tcp**

<b>High (CVSS: 8.1)</b> <b>NVT: UnrealIRCd Authentication Spoofing Vulnerability</b>
<b>Product detection result</b> cpe:/a:unrealircd:unrealircd:3.2.8.1 Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)
<b>Summary</b> UnrealIRCd is prone to authentication spoofing vulnerability.
<b>Vulnerability Detection Result</b> Installed version: 3.2.8.1 Fixed version: 3.2.10.7
<b>Impact</b> Successful exploitation of this vulnerability will allow remote attackers to spoof certificate fingerprints and consequently log in as another user.
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.
<b>Affected Software/OS</b> UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.
<b>Vulnerability Insight</b> The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: UnrealIRCd Authentication Spoofing Vulnerability OID:1.3.6.1.4.1.25623.1.0.809883 Version used: 2023-07-14T16:09:27Z
<b>Product Detection Result</b> Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection OID: 1.3.6.1.4.1.25623.1.0.809884)
<b>References</b> cve: CVE-2016-7144 url: <a href="http://seclists.org/oss-sec/2016/q3/420">http://seclists.org/oss-sec/2016/q3/420</a> url: <a href="http://www.securityfocus.com/bid/92763">http://www.securityfocus.com/bid/92763</a> url: <a href="http://www.openwall.com/lists/oss-security/2016/09/05/8">http://www.openwall.com/lists/oss-security/2016/09/05/8</a> url: <a href="https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b">https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b</a> ... continues on next page ...

...continued from previous page...

↔c50ba1a34a766

url: [https://bugs.unrealircd.org/main\\_page.php](https://bugs.unrealircd.org/main_page.php)**High (CVSS: 7.5)****NVT: UnrealIRCd Backdoor****Summary**

Detection of backdoor in UnrealIRCd.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Solution:****Solution type:** VendorFix

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

**Affected Software/OS**

The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.

**Vulnerability Insight**

Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.

**Vulnerability Detection Method**

Details: UnrealIRCd Backdoor

OID:1.3.6.1.4.1.25623.1.0.80111

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

**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>[\[ return to 192.168.50.239 \]](#)**2.1.14 High 513/tcp**

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

[\[ return to 192.168.50.239 \]](#)

### 2.1.15 High general/tcp

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

...continued from previous page ...	
CPE:	cpe:/o:canonical:ubuntu_linux:8.04
Installed version,	
build or SP:	8.04
EOL date:	2013-05-09
EOL info:	https://wiki.ubuntu.com/Releases
<b>Impact</b> An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.	
<b>Solution:</b> <b>Solution type:</b> Mitigation Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.	
<b>Vulnerability Detection Method</b> Checks if an EOL version of an OS is present on the target host. Details: Operating System (OS) End of Life (EOL) Detection OID:1.3.6.1.4.1.25623.1.0.103674 Version used: 2022-04-05T13:00:52Z	
<b>Product Detection Result</b> Product: cpe:/o:canonical:ubuntu_linux:8.04 Method: OS Detection Consolidation and Reporting OID: 1.3.6.1.4.1.25623.1.0.105937)	

[ [return to 192.168.50.239](#) ]

### 2.1.16 Medium 23/tcp

Medium (CVSS: 4.8) NVT: Telnet Unencrypted Cleartext Login
<b>Summary</b> The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.
<b>Solution:</b> ... continues on next page ...

...continued from previous page ...

**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: 2023-07-20T05:05:17Z

[\[ return to 192.168.50.239 \]](#)

**2.1.17 Medium 5432/tcp**

Medium (CVSS: 5.9)

NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Summary**

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

**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**

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 information.

**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)

... continues on next page ...



...continued from previous page ...
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)
<b>Vulnerability Detection Method</b> Check the used SSL protocols of the services provided by this system. Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012 Version used: 2021-10-15T12:51:02Z
<b>References</b> cve: CVE-2016-0800 cve: CVE-2014-3566 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://drownattack.com/">https://drownattack.com/</a> url: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-report-2014 cert-bund: WID-SEC-2023-0431 cert-bund: WID-SEC-2023-0427 cert-bund: CB-K18/0094 cert-bund: CB-K17/1198 cert-bund: CB-K17/1196 cert-bund: CB-K16/1828 cert-bund: CB-K16/1438 cert-bund: CB-K16/1384 cert-bund: CB-K16/1141 cert-bund: CB-K16/1107 cert-bund: CB-K16/1102 cert-bund: CB-K16/0792 cert-bund: CB-K16/0599 cert-bund: CB-K16/0597 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
...continues on next page ...

...continued from previous page ...

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  
 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

...continues on next page ...

...continued from previous page ...

```

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**

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.

**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)

...continues on next page ...

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

Medium (CVSS: 5.0) NVT: SSL/TLS: Report Weak Cipher Suites	
<b>Summary</b>	This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
<b>Vulnerability Detection Result</b>	'Weak' cipher suites accepted by this service via the SSLv3 protocol: TLS_RSA_WITH_RC4_128_SHA 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_SHA
<b>Solution:</b>	
<b>Solution type:</b> Mitigation	The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.
<b>Vulnerability Insight</b>	... continues on next page ...

...continued from previous page ...
<p>These rules are applied for the evaluation of the cryptographic strength:</p> <ul style="list-style-type: none"> <li>- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)</li> <li>- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)</li> <li>- 1024 bit RSA authentication is considered to be insecure and therefore as weak</li> <li>- Any cipher considered to be secure for only the next 10 years is considered as medium</li> <li>- Any other cipher is considered as strong</li> </ul>
<p><b>Vulnerability Detection Method</b>  Details: SSL/TLS: Report Weak Cipher Suites  OID:1.3.6.1.4.1.25623.1.0.103440  Version used: 2021-12-01T13:10:37Z</p>
<p><b>References</b>  cve: CVE-2013-2566  cve: CVE-2015-2808  cve: CVE-2015-4000  url: <a href="https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↪465_update_6.html">https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↪465_update_6.html</a>  url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a>  url: <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a>  cert-bund: CB-K21/0067  cert-bund: CB-K19/0812  cert-bund: CB-K17/1750  cert-bund: CB-K16/1593  cert-bund: CB-K16/1552  cert-bund: CB-K16/1102  cert-bund: CB-K16/0617  cert-bund: CB-K16/0599  cert-bund: CB-K16/0168  cert-bund: CB-K16/0121  cert-bund: CB-K16/0090  cert-bund: CB-K16/0030  cert-bund: CB-K15/1751  cert-bund: CB-K15/1591  cert-bund: CB-K15/1550  cert-bund: CB-K15/1517  cert-bund: CB-K15/1514  cert-bund: CB-K15/1464  cert-bund: CB-K15/1442  cert-bund: CB-K15/1334  cert-bund: CB-K15/1269  cert-bund: CB-K15/1136  cert-bund: CB-K15/1090  cert-bund: CB-K15/1059  cert-bund: CB-K15/1022  cert-bund: CB-K15/1015</p>
...continues on next page ...

...continued from previous page ...

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-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

...continues on next page ...

...continued from previous page ...

```

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: 5.0)

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.

**Vulnerability Detection Result**

The following indicates that the remote SSL/TLS service is affected:

Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an  
 ↳ existing / already established SSL/TLS connection

-----  
 ↳-----  
 TLSv1.0 | 10

**Impact**

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

**Solution:**

**Solution type:** VendorFix

Users should contact their vendors for specific patch information.

A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

... continues on next page ...

...continued from previous page ...
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
<b>Vulnerability Insight</b> The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: > It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.
<b>Vulnerability Detection Method</b> Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 Version used: 2021-11-15T10:28:20Z
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://orchilles.com/ssl-renegotiation-dos/">https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> 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-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
<b>Summary</b> The remote server's SSL/TLS certificate has already expired.
<b>Vulnerability Detection Result</b> ... continues on next page ...



...continued from previous page...	
<p>The certificate of the remote service expired on 2010-04-16 14:07:45.</p> <p>Certificate details:</p> <pre> 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 </pre>	
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>Replace the SSL/TLS certificate by a new one.</p>	
<p><b>Vulnerability Insight</b></p> <p>This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.</p>	
<p><b>Vulnerability Detection Method</b></p> <p>Details: SSL/TLS: Certificate Expired</p> <p>OID:1.3.6.1.4.1.25623.1.0.103955</p> <p>Version used: 2021-11-22T15:32:39Z</p>	
<p>Medium (CVSS: 4.3)</p> <p>NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p>	
<p><b>Summary</b></p> <p>It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.</p>	
<p><b>Vulnerability Detection Result</b></p> <p>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.</p>	
...continues on next page...	

...continued from previous page ...
<p><b>Impact</b></p> <p>An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.</p>
<p><b>Affected Software/OS</b></p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p><b>Vulnerability Insight</b></p> <p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> <li>- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)</li> <li>- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2021-07-19T08:11:48Z</p>
<p><b>References</b></p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a></p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a></p> <p>url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a></p> <p>url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a></p> <p>url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a></p> <p>↔-report-2014</p> <p>cert-bund: WID-SEC-2023-1435</p> <p>cert-bund: CB-K18/0799</p> <p>cert-bund: CB-K16/1289</p> <p>cert-bund: CB-K16/1096</p> <p>cert-bund: CB-K15/1751</p> <p>cert-bund: CB-K15/1266</p> <p>cert-bund: CB-K15/0850</p> <p>cert-bund: CB-K15/0764</p>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0720  
 cert-bund: CB-K15/0548  
 cert-bund: CB-K15/0526  
 cert-bund: CB-K15/0509  
 cert-bund: CB-K15/0493  
 cert-bund: CB-K15/0384  
 cert-bund: CB-K15/0365  
 cert-bund: CB-K15/0364  
 cert-bund: CB-K15/0302  
 cert-bund: CB-K15/0192  
 cert-bund: CB-K15/0079  
 cert-bund: CB-K15/0016  
 cert-bund: CB-K14/1342  
 cert-bund: CB-K14/0231  
 cert-bund: CB-K13/0845  
 cert-bund: CB-K13/0796  
 cert-bund: CB-K13/0790  
 dfn-cert: DFN-CERT-2020-0177  
 dfn-cert: DFN-CERT-2020-0111  
 dfn-cert: DFN-CERT-2019-0068  
 dfn-cert: DFN-CERT-2018-1441  
 dfn-cert: DFN-CERT-2018-1408  
 dfn-cert: DFN-CERT-2016-1372  
 dfn-cert: DFN-CERT-2016-1164  
 dfn-cert: DFN-CERT-2016-0388  
 dfn-cert: DFN-CERT-2015-1853  
 dfn-cert: DFN-CERT-2015-1332  
 dfn-cert: DFN-CERT-2015-0884  
 dfn-cert: DFN-CERT-2015-0800  
 dfn-cert: DFN-CERT-2015-0758  
 dfn-cert: DFN-CERT-2015-0567  
 dfn-cert: DFN-CERT-2015-0544  
 dfn-cert: DFN-CERT-2015-0530  
 dfn-cert: DFN-CERT-2015-0396  
 dfn-cert: DFN-CERT-2015-0375  
 dfn-cert: DFN-CERT-2015-0374  
 dfn-cert: DFN-CERT-2015-0305  
 dfn-cert: DFN-CERT-2015-0199  
 dfn-cert: DFN-CERT-2015-0079  
 dfn-cert: DFN-CERT-2015-0021  
 dfn-cert: DFN-CERT-2014-1414  
 dfn-cert: DFN-CERT-2013-1847  
 dfn-cert: DFN-CERT-2013-1792  
 dfn-cert: DFN-CERT-2012-1979  
 dfn-cert: DFN-CERT-2012-1829  
 dfn-cert: DFN-CERT-2012-1530  
 dfn-cert: DFN-CERT-2012-1380

...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2012-1377  
dfn-cert: DFN-CERT-2012-1292  
dfn-cert: DFN-CERT-2012-1214  
dfn-cert: DFN-CERT-2012-1213  
dfn-cert: DFN-CERT-2012-1180  
dfn-cert: DFN-CERT-2012-1156  
dfn-cert: DFN-CERT-2012-1155  
dfn-cert: DFN-CERT-2012-1039  
dfn-cert: DFN-CERT-2012-0956  
dfn-cert: DFN-CERT-2012-0908  
dfn-cert: DFN-CERT-2012-0868  
dfn-cert: DFN-CERT-2012-0867  
dfn-cert: DFN-CERT-2012-0848  
dfn-cert: DFN-CERT-2012-0838  
dfn-cert: DFN-CERT-2012-0776  
dfn-cert: DFN-CERT-2012-0722  
dfn-cert: DFN-CERT-2012-0638  
dfn-cert: DFN-CERT-2012-0627  
dfn-cert: DFN-CERT-2012-0451  
dfn-cert: DFN-CERT-2012-0418  
dfn-cert: DFN-CERT-2012-0354  
dfn-cert: DFN-CERT-2012-0234  
dfn-cert: DFN-CERT-2012-0221  
dfn-cert: DFN-CERT-2012-0177  
dfn-cert: DFN-CERT-2012-0170  
dfn-cert: DFN-CERT-2012-0146  
dfn-cert: DFN-CERT-2012-0142  
dfn-cert: DFN-CERT-2012-0126  
dfn-cert: DFN-CERT-2012-0123  
dfn-cert: DFN-CERT-2012-0095  
dfn-cert: DFN-CERT-2012-0051  
dfn-cert: DFN-CERT-2012-0047  
dfn-cert: DFN-CERT-2012-0021  
dfn-cert: DFN-CERT-2011-1953  
dfn-cert: DFN-CERT-2011-1946  
dfn-cert: DFN-CERT-2011-1844  
dfn-cert: DFN-CERT-2011-1826  
dfn-cert: DFN-CERT-2011-1774  
dfn-cert: DFN-CERT-2011-1743  
dfn-cert: DFN-CERT-2011-1738  
dfn-cert: DFN-CERT-2011-1706  
dfn-cert: DFN-CERT-2011-1628  
dfn-cert: DFN-CERT-2011-1627  
dfn-cert: DFN-CERT-2011-1619  
dfn-cert: DFN-CERT-2011-1482

Medium (CVSS: 4.0) NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
<p><b>Summary</b></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><b>Vulnerability Detection Result</b></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><b>Solution:</b></p> <p><b>Solution type:</b> 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><b>Vulnerability Insight</b></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"> <li>- Secure Hash Algorithm 1 (SHA-1)</li> <li>- Message Digest 5 (MD5)</li> <li>- Message Digest 4 (MD4)</li> <li>- Message Digest 2 (MD2)</li> </ul> <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><b>Vulnerability Detection Method</b></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> <p>Version used: 2021-10-15T11:13:32Z</p>
<p><b>References</b></p> <p>url: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-</a>  ... continues on next page ...</p>

...continued from previous page ...

↪sha-1-based-signature-algorithms/

Medium (CVSS: 4.0)

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

**Summary**

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

**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 (see the references).

For Apache Web Servers: Beginning with version 2.4.7, mod\_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

**Vulnerability Insight**

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

**Vulnerability Detection Method**

Checks the DHE temporary public key size.

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

↪..

OID:1.3.6.1.4.1.25623.1.0.106223

Version used: 2023-07-21T05:05:22Z

**References**

url: <https://weakdh.org/>

url: <https://weakdh.org/sysadmin.html>

[ [return to 192.168.50.239](#) ]

**2.1.18 Medium 5900/tcp**

Medium (CVSS: 4.8) NVT: VNC Server Unencrypted Data Transmission
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> The VNC server provides the following insecure or cryptographically weak Security Type(s): 2 (VNC authentication)
<b>Impact</b> An attacker can uncover sensitive data by sniffing traffic to the VNC server.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Vulnerability Detection Method</b> Details: VNC Server Unencrypted Data Transmission OID:1.3.6.1.4.1.25623.1.0.108529 Version used: 2023-07-12T05:05:04Z
<b>References</b> url: <a href="https://tools.ietf.org/html/rfc6143#page-10">https://tools.ietf.org/html/rfc6143#page-10</a>

[ [return to 192.168.50.239](#) ]

### 2.1.19 Medium 22/tcp

Medium (CVSS: 5.3)	
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	
<b>Summary</b> The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).	
<b>Vulnerability Detection Result</b> The remote SSH server supports the following weak KEX algorithm(s):	
KEX algorithm	Reason
-----	
↩-----	
diffie-hellman-group-exchange-sha1	Using SHA-1
diffie-hellman-group1-sha1	Using Oakley Group 2 (a 1024-bit MODP group)
... continues on next page ...	

...continued from previous page ...	
↔) and SHA-1	
<b>Impact</b> An attacker can quickly break individual connections.	
<b>Solution:</b> <b>Solution type:</b> 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.	
<b>Vulnerability Insight</b> - 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.	
<b>Vulnerability Detection Method</b> 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: 2022-12-08T10:12:32Z	
<b>References</b> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a> url: <a href="https://www.rfc-editor.org/rfc/rfc9142.html">https://www.rfc-editor.org/rfc/rfc9142.html</a> url: <a href="https://www.rfc-editor.org/rfc/rfc9142.html#name-summary-guidance-for-imple">https://www.rfc-editor.org/rfc/rfc9142.html#name-summary-guidance-for-imple</a> ↔m url: <a href="https://datatracker.ietf.org/doc/html/rfc6194">https://datatracker.ietf.org/doc/html/rfc6194</a>	

Medium (CVSS: 5.3)	
NVT: Weak Host Key Algorithm(s) (SSH)	
<b>Summary</b> The remote SSH server is configured to allow / support weak host key algorithm(s).	
<b>Vulnerability Detection Result</b> The remote SSH server supports the following weak host key algorithm(s): host key algorithm   Description	
...continues on next page ...	



...continued from previous page ...	
----- ↪-----	
ssh-dss	Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the reported weak host key algorithm(s).	
<b>Vulnerability Detection Method</b> Checks the supported host key algorithms of the remote SSH server. Currently weak host key algorithms are defined as the following: - ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS) Details: Weak Host Key Algorithm(s) (SSH) OID:1.3.6.1.4.1.25623.1.0.117687 Version used: 2021-11-24T06:31:19Z	

Medium (CVSS: 4.3)	
NVT: Weak Encryption Algorithm(s) Supported (SSH)	
<b>Summary</b> The remote SSH server is configured to allow / support weak encryption algorithm(s).	
<b>Vulnerability Detection Result</b> 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	
... continues on next page ...	

...continued from previous page ...
blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the reported weak encryption algorithm(s).
<b>Vulnerability Insight</b> - 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.
<b>Vulnerability Detection Method</b> 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: 2022-12-09T10:11:04Z
<b>References</b> url: <a href="https://www.rfc-editor.org/rfc/rfc4253#section-6.3">https://www.rfc-editor.org/rfc/rfc4253#section-6.3</a> url: <a href="https://www.kb.cert.org/vuls/id/958563">https://www.kb.cert.org/vuls/id/958563</a>

[ [return to 192.168.50.239](#) ]

### 2.1.20 Medium 25/tcp

Medium (CVSS: 6.8) NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability
<b>Summary</b> Multiple vendors' implementations of 'STARTTLS' are prone to a vulnerability that lets attackers inject arbitrary commands.
<b>Vulnerability Detection Result</b> ... continues on next page ...

...continued from previous page ...
Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> An attacker can exploit this issue to execute arbitrary commands in the context of the user running the application. Successful exploits can allow attackers to obtain email usernames and passwords.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> The following vendors are known to be affected: Ipswitch Kerio Postfix Qmail-TLS Oracle SCO Group spamdyke ISC
<b>Vulnerability Detection Method</b> Send a special crafted 'STARTTLS' request and check the response. Details: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection . ↪.. OID:1.3.6.1.4.1.25623.1.0.103935 Version used: 2022-04-14T11:24:11Z
<b>References</b> 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: <a href="http://www.securityfocus.com/bid/46767">http://www.securityfocus.com/bid/46767</a> url: <a href="http://kolab.org/pipermail/kolab-announce/2011/000101.html">http://kolab.org/pipermail/kolab-announce/2011/000101.html</a> url: <a href="http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424">http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424</a> url: <a href="http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7">http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7</a> url: <a href="http://www.kb.cert.org/vuls/id/MAPG-8D9M4P">http://www.kb.cert.org/vuls/id/MAPG-8D9M4P</a> url: <a href="http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-notes.txt">http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-no ↪tes.txt</a> url: <a href="http://www.postfix.org/CVE-2011-0411.html">http://www.postfix.org/CVE-2011-0411.html</a>
... continues on next page ...

...continued from previous page...

```

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

**Summary**

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

**Vulnerability Detection Result**

In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and SSLv3 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256.23.1.0.802067) 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><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.</p>
<p><b>Affected Software/OS</b></p> <p>All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.</p>
<p><b>Vulnerability Insight</b></p> <p>The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> <li>- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)</li> <li>- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check 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: 2021-10-15T12:51:02Z</p>
<p><b>References</b></p> <p>cve: CVE-2016-0800</p> <p>cve: CVE-2014-3566</p> <p>url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a></p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://drownattack.com/">https://drownattack.com/</a></p> <p>url: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a></p> <p>url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a></p> <p>↔-report-2014</p> <p>cert-bund: WID-SEC-2023-0431</p> <p>cert-bund: WID-SEC-2023-0427</p> <p>cert-bund: CB-K18/0094</p> <p>cert-bund: CB-K17/1198</p> <p>cert-bund: CB-K17/1196</p> <p>cert-bund: CB-K16/1828</p> <p>cert-bund: CB-K16/1438</p> <p>cert-bund: CB-K16/1384</p> <p>cert-bund: CB-K16/1141</p> <p>cert-bund: CB-K16/1107</p> <p>cert-bund: CB-K16/1102</p> <p>cert-bund: CB-K16/0792</p>
... continues on next page ...

...continued from previous page ...

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  
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

...continues on next page ...

...continued from previous page ...

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  
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

...continues on next page ...

...continued from previous page ...

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.

**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 bits.

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](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.

... continues on next page ...



...continued from previous page ...	
<b>Vulnerability Detection Result</b> The following indicates that the remote SSL/TLS service is affected: Protocol Version   Successful re-done SSL/TLS handshakes (Renegotiation) over an ↔ existing / already established SSL/TLS connection ----- ↔----- TLSv1.0   10	
<b>Impact</b> The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.	
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.	
<b>Vulnerability Insight</b> The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: > It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.	
<b>Vulnerability Detection Method</b> Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 Version used: 2021-11-15T10:28:20Z	
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://orchilles.com/ssl-renegotiation-dos/">https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a>	
... 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-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

**Summary**

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

**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
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**

... continues on next page ...

...continued from previous page ...
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2021-11-22T15:32:39Z

Medium (CVSS: 5.0) NVT: Check if Mailserver answer to VRFY and EXPN requests
<b>Summary</b> The Mailserver on this host answers to VRFY and/or EXPN requests.
<b>Vulnerability Detection Result</b> 'VRFY root' produces the following answer: 252 2.0.0 root
<b>Solution:</b> <b>Solution type:</b> Workaround Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
<b>Vulnerability Insight</b> VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.
<b>Vulnerability Detection Method</b> Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: 2023-07-12T05:05:04Z
<b>References</b> url: <a href="http://cr.yp.to/smtp/vrfy.html">http://cr.yp.to/smtp/vrfy.html</a>

Medium (CVSS: 4.3) NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
... continues on next page ...

...continued from previous page ...
<b>Vulnerability Detection Result</b> The service is only providing the deprecated TLSv1.0 protocol and supports one o ↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S ↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
<b>Impact</b> An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
<b>Solution:</b> <b>Solution type:</b> Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
<b>Vulnerability Detection Method</b> Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2021-07-19T08:11:48Z
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↪-report-2014 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K18/0799 cert-bund: CB-K16/1289 cert-bund: CB-K16/1096
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/1751  
 cert-bund: CB-K15/1266  
 cert-bund: CB-K15/0850  
 cert-bund: CB-K15/0764  
 cert-bund: CB-K15/0720  
 cert-bund: CB-K15/0548  
 cert-bund: CB-K15/0526  
 cert-bund: CB-K15/0509  
 cert-bund: CB-K15/0493  
 cert-bund: CB-K15/0384  
 cert-bund: CB-K15/0365  
 cert-bund: CB-K15/0364  
 cert-bund: CB-K15/0302  
 cert-bund: CB-K15/0192  
 cert-bund: CB-K15/0079  
 cert-bund: CB-K15/0016  
 cert-bund: CB-K14/1342  
 cert-bund: CB-K14/0231  
 cert-bund: CB-K13/0845  
 cert-bund: CB-K13/0796  
 cert-bund: CB-K13/0790  
 dfn-cert: DFN-CERT-2020-0177  
 dfn-cert: DFN-CERT-2020-0111  
 dfn-cert: DFN-CERT-2019-0068  
 dfn-cert: DFN-CERT-2018-1441  
 dfn-cert: DFN-CERT-2018-1408  
 dfn-cert: DFN-CERT-2016-1372  
 dfn-cert: DFN-CERT-2016-1164  
 dfn-cert: DFN-CERT-2016-0388  
 dfn-cert: DFN-CERT-2015-1853  
 dfn-cert: DFN-CERT-2015-1332  
 dfn-cert: DFN-CERT-2015-0884  
 dfn-cert: DFN-CERT-2015-0800  
 dfn-cert: DFN-CERT-2015-0758  
 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

...continues on next page ...

...continued from previous page ...

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

...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2011-1619  
 dfn-cert: DFN-CERT-2011-1482

Medium (CVSS: 4.3)

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

**Summary**

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

**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:**

**Solution type:** VendorFix

- Remove support for 'RSA\_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**

- Hosts accepting 'RSA\_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**

Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**

Check previous collected cipher suites saved in the KB.

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

OID:1.3.6.1.4.1.25623.1.0.805142

Version used: 2023-07-25T05:05:58Z

... continues on next page ...

...continued from previous page...

**References**

cve: CVE-2015-0204  
url: <https://freakattack.com>  
url: <http://www.securityfocus.com/bid/71936>  
url: <http://secpod.org/blog/?p=3818>  
url: <http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html>  
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: 4.0) NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
<b>Summary</b> The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
<b>Vulnerability Detection Result</b> Server Temporary Key Size: 1024 bits
<b>Impact</b> An attacker might be able to decrypt the SSL/TLS communication offline.
<b>Solution:</b> <b>Solution type:</b> Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
<b>Vulnerability Insight</b> The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.
<b>Vulnerability Detection Method</b> Checks the DHE temporary public key size. Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↪... OID:1.3.6.1.4.1.25623.1.0.106223 Version used: 2023-07-21T05:05:22Z
<b>References</b> url: <a href="https://weakdh.org/">https://weakdh.org/</a> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a>

Medium (CVSS: 4.0) NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
<b>Summary</b> The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.
<b>Vulnerability Detection Result</b> The following certificates are part of the certificate chain but using insecure ↪signature algorithms:
... continues on next page ...

...continued from previous page...	
Subject:	1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173 ↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic ↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi ↪ng outside US,C=XX
Signature Algorithm:	sha1WithRSAEncryption
<b>Solution:</b> <b>Solution type:</b> Mitigation Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.	
<b>Vulnerability Insight</b> The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1 or fingerprint1, Fingerprint2	
<b>Vulnerability Detection Method</b> Check which hashing algorithm was used to sign the remote SSL/TLS certificate. Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm OID:1.3.6.1.4.1.25623.1.0.105880 Version used: 2021-10-15T11:13:32Z	
<b>References</b> url: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</a>	

[ [return to 192.168.50.239](#) ]

### 2.1.21 Medium 80/tcp

Medium (CVSS: 6.8) NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10
<b>Summary</b> TWiki is prone to a cross-site request forgery (CSRF) vulnerability.
<b>Vulnerability Detection Result</b> Installed version: 01.Feb.2003 Fixed version: 4.3.2
<b>Impact</b> Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
<b>Solution:</b> <b>Solution type:</b> VendorFix Upgrade to TWiki version 4.3.2 or later.
<b>Affected Software/OS</b> TWiki version prior to 4.3.2
<b>Vulnerability Insight</b> Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.
<b>Vulnerability Detection Method</b> Details: TWiki Cross-Site Request Forgery Vulnerability - Sep10 OID:1.3.6.1.4.1.25623.1.0.801281 Version used: 2023-07-28T16:09:07Z
<b>References</b> cve: CVE-2009-4898 url: <a href="http://www.openwall.com/lists/oss-security/2010/08/03/8">http://www.openwall.com/lists/oss-security/2010/08/03/8</a> url: <a href="http://www.openwall.com/lists/oss-security/2010/08/02/17">http://www.openwall.com/lists/oss-security/2010/08/02/17</a> url: <a href="http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix">http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix</a> url: <a href="http://twiki.org/cgi-bin/view/Codev/DownloadTWiki">http://twiki.org/cgi-bin/view/Codev/DownloadTWiki</a>

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

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

Medium (CVSS: 6.1) NVT: jQuery < 1.9.0 XSS Vulnerability	
<b>Summary</b> jQuery is prone to a cross-site scripting (XSS) vulnerability.	
<b>Vulnerability Detection Result</b> Installed version: 1.3.2 Fixed version: 1.9.0 Installation path / port: /mutillidae/javascript/ddsmoothmenu/jquery.min.js Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info): - Identified file: <a href="http://192.168.50.239/mutillidae/javascript/ddsmoothmenu/jquery.min.js">http://192.168.50.239/mutillidae/javascript/ddsmoothmenu/jquery.min.js</a> - Referenced at: <a href="http://192.168.50.239/mutillidae/">http://192.168.50.239/mutillidae/</a>	
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 1.9.0 or later.	
<b>Affected Software/OS</b> jQuery prior to version 1.9.0.	
<b>Vulnerability Insight</b> ... continues on next page ...	

...continued from previous page ...
<p>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 '&lt;' 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 '&lt;' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.</p>
<p><b>Vulnerability Detection Method</b>  Checks if a vulnerable version is present on the target host.  Details: jQuery &lt; 1.9.0 XSS Vulnerability  OID:1.3.6.1.4.1.25623.1.0.141636  Version used: 2023-07-14T05:06:08Z</p>
<p><b>References</b>  cve: CVE-2012-6708  url: <a href="https://bugs.jquery.com/ticket/11290">https://bugs.jquery.com/ticket/11290</a>  cert-bund: WID-SEC-2022-0673  cert-bund: CB-K22/0045  cert-bund: CB-K18/1131  dfn-cert: DFN-CERT-2023-1197  dfn-cert: DFN-CERT-2020-0590</p>

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

...continued from previous page ...
Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.
<b>Vulnerability Detection Method</b> Details: TWiki Cross-Site Request Forgery Vulnerability OID:1.3.6.1.4.1.25623.1.0.800400 Version used: 2023-07-27T05:05:08Z
<b>References</b> cve: CVE-2009-1339 url: <a href="http://secunia.com/advisories/34880">http://secunia.com/advisories/34880</a> url: <a href="http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258">http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258</a> url: <a href="http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff">http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff</a> ↪-cve-2009-1339.txt

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

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.11213 Version used: 2023-08-01T13:29:10Z
<b>References</b> 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: <a href="http://www.kb.cert.org/vuls/id/288308">http://www.kb.cert.org/vuls/id/288308</a> url: <a href="http://www.securityfocus.com/bid/11604">http://www.securityfocus.com/bid/11604</a> url: <a href="http://www.securityfocus.com/bid/15222">http://www.securityfocus.com/bid/15222</a> url: <a href="http://www.securityfocus.com/bid/19915">http://www.securityfocus.com/bid/19915</a> url: <a href="http://www.securityfocus.com/bid/24456">http://www.securityfocus.com/bid/24456</a> url: <a href="http://www.securityfocus.com/bid/33374">http://www.securityfocus.com/bid/33374</a> url: <a href="http://www.securityfocus.com/bid/36956">http://www.securityfocus.com/bid/36956</a> url: <a href="http://www.securityfocus.com/bid/36990">http://www.securityfocus.com/bid/36990</a> url: <a href="http://www.securityfocus.com/bid/37995">http://www.securityfocus.com/bid/37995</a> url: <a href="http://www.securityfocus.com/bid/9506">http://www.securityfocus.com/bid/9506</a> url: <a href="http://www.securityfocus.com/bid/9561">http://www.securityfocus.com/bid/9561</a> url: <a href="http://www.kb.cert.org/vuls/id/867593">http://www.kb.cert.org/vuls/id/867593</a> url: <a href="https://httpd.apache.org/docs/current/en/mod/core.html#traceenable">https://httpd.apache.org/docs/current/en/mod/core.html#traceenable</a> url: <a href="https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac↵e-verbs/ba-p/784482">https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac↵e-verbs/ba-p/784482</a> url: <a href="https://owasp.org/www-community/attacks/Cross_Site_Tracing">https://owasp.org/www-community/attacks/Cross_Site_Tracing</a> 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: 5.0)

NVT: awiki &lt;= 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.

**Vulnerability Detection Result**

Vulnerable URL: <http://192.168.50.239/mutillidae/index.php?page=/etc/passwd>

... continues on next page ...

...continued from previous page ...
<b>Impact</b> An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host.
<b>Solution:</b> <b>Solution type:</b> WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
<b>Affected Software/OS</b> awiki version 20100125 and prior.
<b>Vulnerability Detection Method</b> Sends a crafted HTTP GET request and checks the response. Details: awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check OID:1.3.6.1.4.1.25623.1.0.103210 Version used: 2022-06-08T09:12:49Z
<b>References</b> url: <a href="https://www.exploit-db.com/exploits/36047/">https://www.exploit-db.com/exploits/36047/</a> url: <a href="http://www.securityfocus.com/bid/49187">http://www.securityfocus.com/bid/49187</a>

Medium (CVSS: 5.0) NVT: QWikiwiki directory traversal vulnerability
<b>Summary</b> The remote host is running QWikiwiki, a Wiki application written in PHP. The remote version of this software contains a validation input flaw which may allow an attacker to use it to read arbitrary files on the remote host with the privileges of the web server.
<b>Vulnerability Detection Result</b> Vulnerable URL: <a href="http://192.168.50.239/mutillidae/index.php?page=../../../../../../../../etc/passwd%00">http://192.168.50.239/mutillidae/index.php?page=../../../../../../../../etc/passwd%00</a>
<b>Solution:</b> <b>Solution type:</b> WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
<b>Vulnerability Detection Method</b> Details: QWikiwiki directory traversal vulnerability
...continues on next page ...



...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.16100 Version used: 2023-08-03T05:05:16Z
<b>References</b> cve: CVE-2005-0283 url: <a href="http://www.securityfocus.com/bid/12163">http://www.securityfocus.com/bid/12163</a>

Medium (CVSS: 5.0) NVT: /doc directory browsable
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> Vulnerable URL: <a href="http://192.168.50.239/doc/">http://192.168.50.239/doc/</a>
<b>Solution:</b> <b>Solution type:</b> Mitigation Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf: <Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory>
<b>Vulnerability Detection Method</b> Details: /doc directory browsable OID:1.3.6.1.4.1.25623.1.0.10056 Version used: 2023-08-01T13:29:10Z
<b>References</b> cve: CVE-1999-0678 url: <a href="http://www.securityfocus.com/bid/318">http://www.securityfocus.com/bid/318</a>

Medium (CVSS: 4.8) NVT: Cleartext Transmission of Sensitive Information via HTTP
<b>Summary</b> The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
<b>Vulnerability Detection Result</b> The following input fields were identified (URL:input name): <a href="http://192.168.50.239/dvwa/login.php">http://192.168.50.239/dvwa/login.php</a> :password <a href="http://192.168.50.239/phpMyAdmin/">http://192.168.50.239/phpMyAdmin/</a> :pma_password ... continues on next page ...

...continued from previous page ...
<a href="http://192.168.50.239/phpMyAdmin/?D=A:pma_password">http://192.168.50.239/phpMyAdmin/?D=A:pma_password</a> <a href="http://192.168.50.239/tikiwiki/tiki-install.php:pass">http://192.168.50.239/tikiwiki/tiki-install.php:pass</a> <a href="http://192.168.50.239/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword">http://192.168.50.239/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword</a>
<b>Impact</b> An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
<b>Solution:</b> <b>Solution type:</b> Workaround Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
<b>Affected Software/OS</b> Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
<b>Vulnerability Detection Method</b> Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password' Details: Cleartext Transmission of Sensitive Information via HTTP OID:1.3.6.1.4.1.25623.1.0.108440 Version used: 2023-07-20T05:05:17Z
<b>References</b> url: <a href="https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management">https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</a> url: <a href="https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure">https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</a> url: <a href="https://cwe.mitre.org/data/definitions/319.html">https://cwe.mitre.org/data/definitions/319.html</a>
Medium (CVSS: 4.3) NVT: jQuery < 1.6.3 XSS Vulnerability
<b>Summary</b> jQuery is prone to a cross-site scripting (XSS) vulnerability.
<b>Vulnerability Detection Result</b> Installed version: 1.3.2 Fixed version: 1.6.3 Installation
... continues on next page ...

...continued from previous page...
<p>path / port: /mutillidae/javascript/ddsmoothmenu/jquery.min.js</p> <p>Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):</p> <ul style="list-style-type: none"> <li>- Identified file: <a href="http://192.168.50.239/mutillidae/javascript/ddsmoothmenu/jquery.min.js">http://192.168.50.239/mutillidae/javascript/ddsmoothmenu/jquery.min.js</a></li> <li>- Referenced at: <a href="http://192.168.50.239/mutillidae/">http://192.168.50.239/mutillidae/</a></li> </ul>
<p><b>Solution:</b></p> <p><b>Solution type:</b> VendorFix</p> <p>Update to version 1.6.3 or later.</p>
<p><b>Affected Software/OS</b></p> <p>jQuery prior to version 1.6.3.</p>
<p><b>Vulnerability Insight</b></p> <p>Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: jQuery &lt; 1.6.3 XSS Vulnerability</p> <p>OID:1.3.6.1.4.1.25623.1.0.141637</p> <p>Version used: 2023-07-14T05:06:08Z</p>
<p><b>References</b></p> <p>cve: CVE-2011-4969</p> <p>url: <a href="https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/">https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/</a></p> <p>cert-bund: CB-K17/0195</p> <p>dfn-cert: DFN-CERT-2017-0199</p> <p>dfn-cert: DFN-CERT-2016-0890</p>

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

...continued from previous page ...
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
<b>Affected Software/OS</b> phpMyAdmin version 3.3.8.1 and prior.
<b>Vulnerability Insight</b> The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.
<b>Vulnerability Detection Method</b> Details: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability OID:1.3.6.1.4.1.25623.1.0.801660 Version used: 2023-07-28T16:09:07Z
<b>References</b> cve: CVE-2010-4480 url: <a href="http://www.exploit-db.com/exploits/15699/">http://www.exploit-db.com/exploits/15699/</a> url: <a href="http://www.vupen.com/english/advisories/2010/3133">http://www.vupen.com/english/advisories/2010/3133</a> dfn-cert: DFN-CERT-2011-0467 dfn-cert: DFN-CERT-2011-0451 dfn-cert: DFN-CERT-2011-0016 dfn-cert: DFN-CERT-2011-0002
Medium (CVSS: 4.3) NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
<b>Product detection result</b> cpe:/a:apache:http_server:2.2.8 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↦ 0.117232)
<b>Summary</b> Apache HTTP Server is prone to a cookie information disclosure vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
... continues on next page ...

...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to Apache HTTP Server version 2.2.22 or later.
<b>Affected Software/OS</b> Apache HTTP Server versions 2.2.0 through 2.2.21.
<b>Vulnerability Insight</b> The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.
<b>Vulnerability Detection Method</b> Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability OID: 1.3.6.1.4.1.25623.1.0.902830 Version used: 2022-04-27T12:01:52Z
<b>Product Detection Result</b> Product: cpe:/a:apache:http_server:2.2.8 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
<b>References</b> cve: CVE-2012-0053 url: <a href="http://secunia.com/advisories/47779">http://secunia.com/advisories/47779</a> url: <a href="http://www.securityfocus.com/bid/51706">http://www.securityfocus.com/bid/51706</a> url: <a href="http://www.exploit-db.com/exploits/18442">http://www.exploit-db.com/exploits/18442</a> url: <a href="http://rhn.redhat.com/errata/RHSA-2012-0128.html">http://rhn.redhat.com/errata/RHSA-2012-0128.html</a> url: <a href="http://httpd.apache.org/security/vulnerabilities_22.html">http://httpd.apache.org/security/vulnerabilities_22.html</a> url: <a href="http://svn.apache.org/viewvc?view=revision&amp;revision=1235454">http://svn.apache.org/viewvc?view=revision&amp;revision=1235454</a> url: <a href="http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html">http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html</a> cert-bund: CB-K15/0080 cert-bund: CB-K14/1505 cert-bund: CB-K14/0608 dfn-cert: DFN-CERT-2015-0082 dfn-cert: DFN-CERT-2014-1592 dfn-cert: DFN-CERT-2014-0635 dfn-cert: DFN-CERT-2013-1307 dfn-cert: DFN-CERT-2012-1276 dfn-cert: DFN-CERT-2012-1112 dfn-cert: DFN-CERT-2012-0928 dfn-cert: DFN-CERT-2012-0758 dfn-cert: DFN-CERT-2012-0744 dfn-cert: DFN-CERT-2012-0568 dfn-cert: DFN-CERT-2012-0425 dfn-cert: DFN-CERT-2012-0424
... continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0387
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
dfn-cert: DFN-CERT-2012-0306
dfn-cert: DFN-CERT-2012-0264
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188
```

[\[ return to 192.168.50.239 \]](#)**2.1.22 Medium 21/tcp**

Medium (CVSS: 6.4)

NVT: Anonymous FTP Login Reporting

**Summary**

Reports if the remote FTP Server allows anonymous logins.

**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**

... continues on next page ...

...continued from previous page ...
Details: Anonymous FTP Login Reporting OID:1.3.6.1.4.1.25623.1.0.900600 Version used: 2021-10-20T09:03:29Z
<b>References</b> cve: CVE-1999-0497

Medium (CVSS: 4.8) NVT: FTP Unencrypted Cleartext Login
<b>Summary</b> The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
<b>Vulnerability Detection Result</b> The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↔. Response(s): Non-anonymous sessions: 331 Please specify the password. Anonymous sessions: 331 Please specify the password.
<b>Impact</b> An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
<b>Solution:</b> <b>Solution type:</b> Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
<b>Vulnerability Detection Method</b> Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108528 Version used: 2023-07-14T16:09:27Z

[\[ return to 192.168.50.239 \]](#)

### 2.1.23 Medium 2121/tcp

Medium (CVSS: 4.8) NVT: FTP Unencrypted Cleartext Login
... continues on next page ...

...continued from previous page ...
<b>Summary</b> The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
<b>Vulnerability Detection Result</b> The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↩. Response(s): Non-anonymous sessions: 331 Password required for openvasvt Anonymous sessions: 331 Password required for anonymous
<b>Impact</b> An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
<b>Solution:</b> <b>Solution type:</b> Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
<b>Vulnerability Detection Method</b> Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108528 Version used: 2023-07-14T16:09:27Z

[ [return to 192.168.50.239](#) ]

#### 2.1.24 Medium 445/tcp

Medium (CVSS: 6.0) NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check
<b>Product detection result</b> cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
<b>Summary</b> Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
... continues on next page ...



...continued from previous page ...
<b>Impact</b> An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the referenced vendor advisory.
<b>Affected Software/OS</b> This issue affects Samba 3.0.0 through 3.0.25rc3.
<b>Vulnerability Detection Method</b> Send a crafted command to the samba server and check for a remote command execution. Details: Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check OID:1.3.6.1.4.1.25623.1.0.108011 Version used: 2023-07-20T05:05:17Z
<b>Product Detection Result</b> Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
<b>References</b> cve: CVE-2007-2447 url: <a href="http://www.securityfocus.com/bid/23972">http://www.securityfocus.com/bid/23972</a> url: <a href="https://www.samba.org/samba/security/CVE-2007-2447.html">https://www.samba.org/samba/security/CVE-2007-2447.html</a>

[ [return to 192.168.50.239](#) ]

### 2.1.25 Low 5432/tcp

Low (CVSS: 3.4) NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
<b>Summary</b> This host is prone to an information disclosure vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> ... continues on next page ...

...continued from previous page ...
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
<b>Solution:</b> <b>Solution type:</b> Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
<b>Vulnerability Insight</b> The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
<b>Vulnerability Detection Method</b> Evaluate previous collected information about this service. Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↪.. OID:1.3.6.1.4.1.25623.1.0.802087 Version used: 2023-07-26T05:05:09Z
<b>References</b> cve: CVE-2014-3566 url: <a href="https://www.openssl.org/~bodo/ssl-poodle.pdf">https://www.openssl.org/~bodo/ssl-poodle.pdf</a> url: <a href="http://www.securityfocus.com/bid/70574">http://www.securityfocus.com/bid/70574</a> url: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a> url: <a href="https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html">https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html</a> url: <a href="http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin-ssl-30.html">http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin-ssl-30.html</a> ↪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
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0384  
 cert-bund: CB-K15/0287  
 cert-bund: CB-K15/0252  
 cert-bund: CB-K15/0246  
 cert-bund: CB-K15/0237  
 cert-bund: CB-K15/0118  
 cert-bund: CB-K15/0110  
 cert-bund: CB-K15/0108  
 cert-bund: CB-K15/0080  
 cert-bund: CB-K15/0078  
 cert-bund: CB-K15/0077  
 cert-bund: CB-K15/0075  
 cert-bund: CB-K14/1617  
 cert-bund: CB-K14/1581  
 cert-bund: CB-K14/1537  
 cert-bund: CB-K14/1479  
 cert-bund: CB-K14/1458  
 cert-bund: CB-K14/1342  
 cert-bund: CB-K14/1314  
 cert-bund: CB-K14/1313  
 cert-bund: CB-K14/1311  
 cert-bund: CB-K14/1304  
 cert-bund: CB-K14/1296  
 dfn-cert: DFN-CERT-2017-1238  
 dfn-cert: DFN-CERT-2017-1236  
 dfn-cert: DFN-CERT-2016-1929  
 dfn-cert: DFN-CERT-2016-1527  
 dfn-cert: DFN-CERT-2016-1468  
 dfn-cert: DFN-CERT-2016-1168  
 dfn-cert: DFN-CERT-2016-0884  
 dfn-cert: DFN-CERT-2016-0642  
 dfn-cert: DFN-CERT-2016-0388  
 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

...continues on next page ...

...continued from previous page ...

```
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 192.168.50.239](#) ]**2.1.26 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

**Vulnerability Detection Result**

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

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

**Solution:**

**Solution type:** Mitigation

Various mitigations are possible:

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

**Vulnerability Insight**

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

**Vulnerability Detection Method**

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

... continues on next page ...

...continued from previous page ...
Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2023-05-11T09:09:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.50.239 \]](#)

### 2.1.27 Low 22/tcp

Low (CVSS: 2.6) NVT: Weak MAC Algorithm(s) Supported (SSH)
<b>Summary</b> The remote SSH server is configured to allow / support weak MAC algorithm(s).
<b>Vulnerability Detection Result</b> The remote SSH server supports the following weak client-to-server MAC algorithm $\hookrightarrow(s)$ : hmac-md5 hmac-md5-96 hmac-sha1-96 The remote SSH server supports the following weak server-to-client MAC algorithm $\hookrightarrow(s)$ : hmac-md5 hmac-md5-96 hmac-sha1-96
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the reported weak MAC algorithm(s).
<b>Vulnerability Detection Method</b> Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - none algorithm
... continues on next page ...

...continued from previous page ...

Details: Weak MAC Algorithm(s) Supported (SSH)  
 OID:1.3.6.1.4.1.25623.1.0.105610  
 Version used: 2021-09-20T11:05:40Z

[ [return to 192.168.50.239](#) ]**2.1.28 Low 25/tcp**

Low (CVSS: 3.7)

NVT: SSL/TLS: 'DHE\_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

**Summary**

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

**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
- If running OpenSSL update to version 1.0.2b or 1.0.1n or later.

**Affected Software/OS**

- Hosts accepting 'DHE\_EXPORT' cipher suites
- OpenSSL version before 1.0.2b and 1.0.1n

**Vulnerability Insight**

Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE\_EXPORT' cipher suites.

**Vulnerability Detection Method**

Check previous collected cipher suites saved in the KB.

Details: SSL/TLS: 'DHE\_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

... continues on next page ...

...continued from previous page...	
OID:1.3.6.1.4.1.25623.1.0.805188	
Version used: 2023-07-25T05:05:58Z	
<b>References</b>	
cve: CVE-2015-4000	
url: <a href="https://weakdh.org">https://weakdh.org</a>	
url: <a href="http://www.securityfocus.com/bid/74733">http://www.securityfocus.com/bid/74733</a>	
url: <a href="https://weakdh.org/imperfect-forward-secrecy.pdf">https://weakdh.org/imperfect-forward-secrecy.pdf</a>	
url: <a href="http://openwall.com/lists/oss-security/2015/05/20/8">http://openwall.com/lists/oss-security/2015/05/20/8</a>	
url: <a href="https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained">https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained</a>	
url: <a href="https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes">https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes</a>	
cert-bund: CB-K21/0067	
cert-bund: CB-K19/0812	
cert-bund: CB-K16/1593	
cert-bund: CB-K16/1552	
cert-bund: CB-K16/0617	
cert-bund: CB-K16/0599	
cert-bund: CB-K16/0168	
cert-bund: CB-K16/0121	
cert-bund: CB-K16/0090	
cert-bund: CB-K16/0030	
cert-bund: CB-K15/1591	
cert-bund: CB-K15/1550	
cert-bund: CB-K15/1517	
cert-bund: CB-K15/1464	
cert-bund: CB-K15/1442	
cert-bund: CB-K15/1334	
cert-bund: CB-K15/1269	
cert-bund: CB-K15/1136	
cert-bund: CB-K15/1090	
cert-bund: CB-K15/1059	
cert-bund: CB-K15/1022	
cert-bund: CB-K15/1015	
cert-bund: CB-K15/0964	
cert-bund: CB-K15/0932	
cert-bund: CB-K15/0927	
cert-bund: CB-K15/0926	
cert-bund: CB-K15/0907	
cert-bund: CB-K15/0901	
cert-bund: CB-K15/0896	
cert-bund: CB-K15/0877	
cert-bund: CB-K15/0834	
cert-bund: CB-K15/0802	
cert-bund: CB-K15/0733	
dfn-cert: DFN-CERT-2021-0775	
dfn-cert: DFN-CERT-2020-1561	
dfn-cert: DFN-CERT-2020-1276	
...continues on next page...	

...continued from previous page ...

```

dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0737

```

Low (CVSS: 3.4)

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

**Summary**

This host is prone to an information disclosure vulnerability.

**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.

... continues on next page ...



...continued from previous page ...	
<b>Solution:</b> <b>Solution type:</b> Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+	
<b>Vulnerability Insight</b> The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code	
<b>Vulnerability Detection Method</b> Evaluate previous collected information about this service. Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↪.. OID:1.3.6.1.4.1.25623.1.0.802087 Version used: 2023-07-26T05:05:09Z	
<b>References</b> cve: CVE-2014-3566 url: <a href="https://www.openssl.org/~bodo/ssl-poodle.pdf">https://www.openssl.org/~bodo/ssl-poodle.pdf</a> url: <a href="http://www.securityfocus.com/bid/70574">http://www.securityfocus.com/bid/70574</a> url: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a> url: <a href="https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html">https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html</a> url: <a href="http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin">http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin</a> ↪g-ssl-30.html cert-bund: WID-SEC-2023-0431 cert-bund: CB-K17/1198 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	
...continues on next page ...	

...continued from previous page ...

cert-bund: CB-K15/0246  
 cert-bund: CB-K15/0237  
 cert-bund: CB-K15/0118  
 cert-bund: CB-K15/0110  
 cert-bund: CB-K15/0108  
 cert-bund: CB-K15/0080  
 cert-bund: CB-K15/0078  
 cert-bund: CB-K15/0077  
 cert-bund: CB-K15/0075  
 cert-bund: CB-K14/1617  
 cert-bund: CB-K14/1581  
 cert-bund: CB-K14/1537  
 cert-bund: CB-K14/1479  
 cert-bund: CB-K14/1458  
 cert-bund: CB-K14/1342  
 cert-bund: CB-K14/1314  
 cert-bund: CB-K14/1313  
 cert-bund: CB-K14/1311  
 cert-bund: CB-K14/1304  
 cert-bund: CB-K14/1296  
 dfn-cert: DFN-CERT-2017-1238  
 dfn-cert: DFN-CERT-2017-1236  
 dfn-cert: DFN-CERT-2016-1929  
 dfn-cert: DFN-CERT-2016-1527  
 dfn-cert: DFN-CERT-2016-1468  
 dfn-cert: DFN-CERT-2016-1168  
 dfn-cert: DFN-CERT-2016-0884  
 dfn-cert: DFN-CERT-2016-0642  
 dfn-cert: DFN-CERT-2016-0388  
 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

...continues on next page ...

...	...continued from previous page ...
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 192.168.50.239](#) ]

### 2.1.29 Low general/tcp

Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 9495502 Packet 2: 9495610
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation 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.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> ... continues on next page ...

...continued from previous page...
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: 2023-08-01T13:29:10Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a>

[\[ return to 192.168.50.239 \]](#)

---

This file was automatically generated.