Scan Report

March 7, 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 "scan webserver". The scan started at Tue Mar 7 01:32:31 2023 UTC and ended at Tue Mar 7 02:30:32 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

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.200.0.12 www.seclab.net	18	38	6	0	0
Total: 1	18	38	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 62 results selected by the filtering described above. Before filtering there were 487 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.200.0.12 - www.seclab.net	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 10.200.0.12

Host scan start	Tue Mar 7 01:33:05 2023 UTC
Host scan end	Tue Mar 7 02:30:25 2023 UTC

Service (Port)	Threat Level
21/tcp	High
8787/tcp	High
1524/tcp	High
3632/tcp	High
512/tcp	High
5432/tcp	High
6200/tcp	High
8009/tcp	High
80/tcp	High

. . . (continues) . . .

... (continued) ...

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

2.1.1 High 21/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

... continues on next page ...

... continued from previous page ...

Details: vsftpd Compromised Source Packages Backdoor Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: 2022-04-28T13:38:57Z

References
url: http://www.securityfocus.com/bid/48539
url: http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdo
↪ored.html
url: https://security.appspot.com/vsftpd.html

[return to 10.200.0.12]

2.1.2 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
↪rbitrary syscall commands on the remote host. Sending an invalid syscall the s
↪ervice returned the following response:
Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in ‘syscall’"0/usr/lib/
↪ruby/1.8/drb/drb.rb:1555:in ‘send’"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in ‘__se
↪nd__’"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in ‘perform_without_block’"3/usr/lib/
↪ruby/1.8/drb/drb.rb:1515:in ‘perform’"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in ‘m
↪ain_loop’"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in ‘loop’"5/usr/lib/ruby/1.8/drb/
↪drb.rb:1585:in ‘main_loop’"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in ‘start’"5/usr
↪/lib/ruby/1.8/drb/drb.rb:1581:in ‘main_loop’"//usr/lib/ruby/1.8/drb/drb.rb:143
↪0:in ‘run’"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in ‘start’"//usr/lib/ruby/1.8/dr
↪b/drb.rb:1427:in ‘run’"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in ‘initialize’"//us
↪r/lib/ruby/1.8/drb/drb.rb:1627:in ‘new’"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
↪‘start_service’"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
↪plemented

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

Solution:

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Method
Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.
Details: `Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.108010
Version used: `2022-04-13T13:17:10Z`

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

[return to 10.200.0.12]

2.1.3 High 1524/tcp

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

Summary
A backdoor is installed on the remote host.

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

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

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details: `Possible Backdoor: Ingreslock`
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: `2020-08-24T08:40:10Z`

[return to 10.200.0.12]

2.1.4 High 3632/tcp

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

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

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

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

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

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

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

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

[return to 10.200.0.12]

2.1.5 High 512/tcp

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

Summary
This remote host is running a rexec service.

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `The rexec service is running`
OID:1.3.6.1.4.1.25623.1.0.100111
Version used: `2020-10-01T11:33:30Z`

References
`cve: CVE-1999-0618`

[return to 10.200.0.12]

2.1.6 High 5432/tcp

High (CVSS: 9.0)
NVT: PostgreSQL weak password

Product detection result
`cpe:/a:postgresql:postgresql:8.3.1`
`Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)`

... continues on next page ...

... continued from previous page ...

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 weak password`
OID:1.3.6.1.4.1.25623.1.0.103552
Version used: `2022-05-31T14:35:19Z`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

High (CVSS: 7.4)
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Summary
OpenSSL is prone to security-bypass vulnerability.

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

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

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method
Send two SSL ChangeCipherSpec request and check the response.
Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105042
Version used: 2022-04-14T11:24:11Z

References
cve: CVE-2014-0224
url: https://www.openssl.org/news/secadv/20140605.txt
url: http://www.securityfocus.com/bid/67899
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

... continues on next page ...

... continued from previous page ...

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

[return to 10.200.0.12]

2.1.7 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

... continues on next page ...

... continued from previous page ...

Version used: 2022-04-28T13:38:57Z

References

url: http://www.securityfocus.com/bid/48539
url: http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdo
↪ored.html
url: https://security.appspot.com/vsftpd.html

[return to 10.200.0.12]

2.1.8 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 \x0002OK  \x0001 \x000CContent-Type  \x001Ctext/html;charset=
↪ISO-8859-1 AB\x001FÃ¼\x0003\x001Fâ<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at
      http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
    <head>
    <title>Apache Tomcat/5.5</title>
    <style type="text/css">
    /*<![CDATA[*/
      body {
```

... continues on next page ...

... continued from previous page ...

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

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

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

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

... continues on next page ...

... continued from previous page ...

```
         text-align: right;
         font-size: 80%;
     }
     /*]]>*/
   </style>
</head>
<body>
<!-- Header -->
<table id="banner" width="100%">
    <tr>
      <td align="left" style="width:130px">
        <a href="http://tomcat.apache.org/">
   <img src="tomcat.gif" height="92" width="130" alt="The Mighty Tomcat - MEOW!"
↪/>
 </a>
      </td>
      <td align="left" valign="top"><b>Apache Tomcat/5.5</b></td>
      <td align="right">
        <a href="http://www.apache.org/">
   <img src="asf-logo-wide.gif" height="51" width="537" alt="The Apache Software
↪ Foundation"/>
 </a>
       </td>
     </tr>
</table>
<table>
    <tr>
        <!-- Table of Contents -->
        <td valign="top">
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
   <th>Administration</th>
                </tr>
                <tr>
   <td class="menu">
     <a href="manager/status">Status</a><br/>
                    <a href="admin">Tomcat Administration</a><br/>
                    <a href="manager/html">Tomcat Manager</a><br/>
                     
                  </td>
                </tr>
            </table>
     <br />
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
   <th>Documentation</th>
                </tr>
```

... continues on next page ...

... continued from previous page ...

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

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

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

... continues on next page ...

... continued from previous page ...

```
                    <a href="webdav/">WebDAV capabilities</a><br/>
           
                  </td>
                </tr>
            </table>

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

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

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

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

... continues on next page ...

... continued from previous page ...

```
            is restricted to users with role "admin". The manager webapp
            is restricted to users with role "manager".</b>
            Users are defined in <code>$CATALINA_HOME/conf/tomcat-users.xml</cod
↪e>.</p>
            <p>Included with this release are a host of sample Servlets and JSPs
↪ (with associated source code), extensive documentation (including the Servlet
↪ 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web app
↪lications.</p>
            <p>Tomcat mailing lists are available at the Tomcat project web site
↪:</p>
           <ul>
               <li><b><a href="mailto:users@tomcat.apache.org">users@tomc
```

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

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

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

Vulnerability Detection Method
Sends a crafted AJP request and checks the response.
Details: `Apache Tomcat AJP RCE Vulnerability (Ghostcat)`
OID:1.3.6.1.4.1.25623.1.0.143545
Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2020-1938
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1
↪a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E
url: https://www.chaitin.cn/en/ghostcat
url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487
url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi
url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances
↪-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/
url: https://tomcat.apache.org/tomcat-7.0-doc/changelog.html
url: https://tomcat.apache.org/tomcat-8.5-doc/changelog.html
```

... continues on next page ...

... continued from previous page ...

```
url: https://tomcat.apache.org/tomcat-9.0-doc/changelog.html
cert-bund: CB-K20/0711
cert-bund: CB-K20/0705
cert-bund: CB-K20/0693
cert-bund: CB-K20/0555
cert-bund: CB-K20/0543
cert-bund: CB-K20/0154
dfn-cert: DFN-CERT-2021-1736
dfn-cert: DFN-CERT-2020-1508
dfn-cert: DFN-CERT-2020-1413
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2020-1134
dfn-cert: DFN-CERT-2020-0850
dfn-cert: DFN-CERT-2020-0835
dfn-cert: DFN-CERT-2020-0821
dfn-cert: DFN-CERT-2020-0569
dfn-cert: DFN-CERT-2020-0557
dfn-cert: DFN-CERT-2020-0501
dfn-cert: DFN-CERT-2020-0381
```

[return to 10.200.0.12]

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.

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Method
Details: `TWiki XSS and Command Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: `2022-05-11T11:17:52Z`

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

High (CVSS: 7.5)
NVT: phpinfo() output Reporting

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

Vulnerability Detection Result
```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://www.seclab.net/mutillidae/phpinfo.php
http://www.seclab.net/phpinfo.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

... continues on next page ...

... continued from previous page ...

Details: phpinfo() output Reporting
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: 2020-08-24T15:18:35Z

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://www.seclab.net/dav/puttest958728487.html
We could delete the following files via the DELETE method at this web server:
http://www.seclab.net/dav/puttest958728487.html

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

Solution:
Solution type: Mitigation
Use access restrictions to these dangerous HTTP methods or disable them completely.

Affected Software/OS
Web servers with enabled PUT and/or DELETE methods.

Vulnerability Detection Method
Checks if dangerous HTTP methods such as PUT and DELETE are enabled and can be misused to upload or delete files.
Details: Test HTTP dangerous methods
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: 2022-05-12T09:32:01Z

References
url: http://www.securityfocus.com/bid/12141
owasp: OWASP-CM-001

High (CVSS: 7.5)
NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

... continues on next page ...

... continued from previous page ...

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result
```
By doing the following HTTP POST request:
"HTTP POST" body : <?php phpinfo();?>
URL              : http://www.seclab.net/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>
```

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

Solution:
Solution type: VendorFix
PHP 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.

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`

... continues on next page ...

... continued from previous page ...

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

[return to 10.200.0.12]

2.1.10 High 5900/tcp

High (CVSS: 9.0)
NVT: VNC Brute Force Login

Summary
Try to log in with given passwords via VNC protocol.

Vulnerability Detection Result
`It was possible to connect to the VNC server with the password: password`

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: Mitigation
Change the password to something hard to guess or enable password protection at all.

Vulnerability Insight
This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all.
Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked.
Note as well that passwords can be max. 8 characters long.

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

[return to 10.200.0.12]

2.1.11 High 2121/tcp

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>`
`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
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.

... continues on next page ...

... continued from previous page ...

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: `2022-08-04T13:37:02Z`

References
`cve: CVE-1999-0501`
`cve: CVE-1999-0502`
`cve: CVE-1999-0507`
`cve: CVE-1999-0508`

[return to 10.200.0.12]

2.1.12 High 6697/tcp

High (CVSS: 8.1)
NVT: UnrealIRCd Authentication Spoofing Vulnerability

Product detection result
`cpe:/a:unrealircd:unrealircd:3.2.8.1`
`Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)`

Summary
UnrealIRCd is prone to authentication spoofing vulnerability.

Vulnerability Detection Result
`Installed version: 3.2.8.1`
`Fixed version: 3.2.10.7`

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

Solution:
Solution type: VendorFix
Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.

Affected Software/OS
UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `UnrealIRCd Authentication Spoofing Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.809883
Version used: `2022-04-13T11:57:07Z`

Product Detection Result
Product: `cpe:/a:unrealircd:unrealircd:3.2.8.1`
Method: `UnrealIRCd Detection`
OID: 1.3.6.1.4.1.25623.1.0.809884)

References
`cve: CVE-2016-7144`
`url: http://seclists.org/oss-sec/2016/q3/420`
`url: http://www.securityfocus.com/bid/92763`
`url: http://www.openwall.com/lists/oss-security/2016/09/05/8`
`url: https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b`
`↪c50ba1a34a766`
`url: https://bugs.unrealircd.org/main_page.php`

[return to 10.200.0.12]

2.1.13 High 1099/tcp

High (CVSS: 7.5)
NVT: Java RMI Server Insecure Default Configuration RCE Vulnerability

Summary
Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code (remote code execution/RCE) on a targeted system with elevated privileges.

Vulnerability Detection Result
`By doing an RMI request it was possible to trigger the vulnerability and make th`
`↪e remote host sending a request back to the scanner host (Details on the recei`
`↪ved packet follows).`
`Destination IP:   10.200.0.10 (receiving IP on scanner host side)`
`Destination port: 16315/tcp (receiving port on scanner host side)`
`Originating IP:   10.200.0.12 (originating IP from target host side)`

Impact

... continues on next page ...

... continued from previous page ...

An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.

Solution:
Solution type: Workaround
Disable class-loading. Please contact the vendor of the affected system for additional guidance.

Vulnerability Insight
The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software.

Vulnerability Detection Method
Sends a crafted JRMI request and checks if the target 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`

References
`cve: CVE-2011-3556`
`url: https://web.archive.org/web/20211208040855/http://www.securitytracker.com/i`
`↪d?1026215`
`url: https://web.archive.org/web/20110824060234/http://download.oracle.com/javas`
`↪e/1.3/docs/guide/rmi/spec/rmi-protocol.html`
`url: https://tools.cisco.com/security/center/viewAlert.x?alertId=23665`
`dfn-cert: DFN-CERT-2012-1829`
`dfn-cert: DFN-CERT-2012-1380`
`dfn-cert: DFN-CERT-2012-1377`
`dfn-cert: DFN-CERT-2012-1156`
`dfn-cert: DFN-CERT-2012-1155`
`dfn-cert: DFN-CERT-2012-0956`
`dfn-cert: DFN-CERT-2012-0828`
`dfn-cert: DFN-CERT-2012-0815`
`dfn-cert: DFN-CERT-2012-0638`
`dfn-cert: DFN-CERT-2012-0451`
`dfn-cert: DFN-CERT-2012-0418`
`dfn-cert: DFN-CERT-2012-0354`
`dfn-cert: DFN-CERT-2012-0146`
`dfn-cert: DFN-CERT-2012-0142`
`dfn-cert: DFN-CERT-2012-0126`
`dfn-cert: DFN-CERT-2012-0095`
`dfn-cert: DFN-CERT-2012-0047`

... continues on next page ...

... continued from previous page ...

```
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 10.200.0.12]

2.1.14 High general/tcp

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

Product detection result

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

Summary

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

Vulnerability Detection Result

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

Impact

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

Solution:

Solution type: Mitigation

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

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

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`

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

[return to 10.200.0.12]

2.1.15 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.

... continues on next page ...

... continued from previous page ...

Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Vulnerability Detection Method
Details: `Anonymous FTP Login Reporting`
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: `2021-10-20T09:03:29Z`

References
`cve: CVE-1999-0497`

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

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

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Please specify the password.
Anonymous sessions:     331 Please specify the password.
```

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

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

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2020-08-24T08:40:10Z`

[return to 10.200.0.12]

2.1.16 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

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

Vulnerability Detection Result

```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
-------------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2021-11-24T06:31:19Z`

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

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

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-------------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation

. . . continues on next page . . .

... continued from previous page ...

Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally 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`

References
`url: https://weakdh.org/sysadmin.html`
`url: https://www.rfc-editor.org/rfc/rfc9142.html`
`url: https://www.rfc-editor.org/rfc/rfc9142.html#name-summary-guidance-for-imple`
`↪m`
`url: https://datatracker.ietf.org/doc/html/rfc6194`

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

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

Vulnerability Detection Result
`The remote SSH server supports the following weak client-to-server encryption al`
`↪gorithm(s):`
`3des-cbc`
`aes128-cbc`
`aes192-cbc`
`aes256-cbc`
`arcfour`
`arcfour128`
`arcfour256`

... continues on next page ...

... continued from previous page ...

```
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Vulnerability Insight
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- none algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2022-12-09T10:11:04Z`

References
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`
`url: https://www.kb.cert.org/vuls/id/958563`

[return to 10.200.0.12]

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 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.
```

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)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

Vulnerability Detection Method
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`

References
```
cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
```

... continues on next page ...

... continued from previous page ...

```
url: https://drownattack.com/
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254

... continues on next page ...

... continued from previous page ...

```
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 w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D
↪626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for C
↪omplication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no su
↪ch thing outside US,C=XX (Server certificate)
```

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

Solution:
Solution type: Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

Vulnerability Insight
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.

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

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

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
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.

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
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

References
cve: CVE-2013-2566

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
```

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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: 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
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955

... continues on next page ...

... continued from previous page ...

Version used: 2021-11-22T15:32:39Z

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.

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

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: 2021-11-15T10:28:20Z

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://orchilles.com/ssl-renegotiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
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: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary

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

Vulnerability Detection Result

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.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:

Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
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`

References
`cve: CVE-2015-0204`
`cve: CVE-2011-3389`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`
`cert-bund: CB-K15/0526`
`cert-bund: CB-K15/0509`
`cert-bund: CB-K15/0493`
`cert-bund: CB-K15/0384`
`cert-bund: CB-K15/0365`
`cert-bund: CB-K15/0364`
`cert-bund: CB-K15/0302`
`cert-bund: CB-K15/0192`
`cert-bund: CB-K15/0079`
`cert-bund: CB-K15/0016`
`cert-bund: CB-K14/1342`
`cert-bund: CB-K14/0231`
`cert-bund: CB-K13/0845`
`cert-bund: CB-K13/0796`
`cert-bund: CB-K13/0790`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
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

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

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

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).

... continues on next page ...

... continued from previous page ...

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 Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2021-02-12T06:42:15Z`

References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

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

Vulnerability Detection Result
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
Signature Algorithm:  sha1WithRSAEncryption
```

Solution:
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

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

[return to 10.200.0.12]

2.1.18 Medium 445/tcp

Medium (CVSS: 6.0)
NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check

Product detection result
`cpe:/a:samba:samba:3.0.20`
`Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)`

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

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

Impact

... continues on next page ...

... continued from previous page ...

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

Solution:
Solution type: VendorFix
Updates are available. Please see the referenced vendor advisory.

Affected Software/OS
This issue affects Samba 3.0.0 through 3.0.25rc3.

Vulnerability Detection Method
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: `2022-12-05T10:11:03Z`

Product Detection Result
Product: `cpe:/a:samba:samba:3.0.20`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
`cve: CVE-2007-2447`
`url: http://www.securityfocus.com/bid/23972`
`url: https://www.samba.org/samba/security/CVE-2007-2447.html`

[return to 10.200.0.12]

2.1.19 Medium 25/tcp

Medium (CVSS: 6.8)
NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability

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

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

Impact

... continues on next page ...

... continued from previous page ...

An attacker can exploit this issue to execute arbitrary commands in the context of the user running the application. Successful exploits can allow attackers to obtain email usernames and passwords.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
The following vendors are known to be affected:
Ipswitch
Kerio
Postfix
Qmail-TLS
Oracle
SCO Group
spamdyke
ISC

Vulnerability Detection Method
Send a special crafted 'STARTTLS' request and check the response.
Details: `Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.103935
Version used: `2022-04-14T11:24:11Z`

References
`cve: CVE-2011-0411`
`cve: CVE-2011-1430`
`cve: CVE-2011-1431`
`cve: CVE-2011-1432`
`cve: CVE-2011-1506`
`cve: CVE-2011-1575`
`cve: CVE-2011-1926`
`cve: CVE-2011-2165`
`url: http://www.securityfocus.com/bid/46767`
`url: http://kolab.org/pipermail/kolab-announce/2011/000101.html`
`url: http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424`
`url: http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7`
`url: http://www.kb.cert.org/vuls/id/MAPG-8D9M4P`
`url: http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-no`
`↪tes.txt`
`url: http://www.postfix.org/CVE-2011-0411.html`
`url: http://www.pureftpd.org/project/pure-ftpd/news`
`url: http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes`
`↪_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf`

... continues on next page ...

... continued from previous page ...

```
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 S
↪SLv3 protocols and supports one or more ciphers. Those supported ciphers can b
↪e found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256
↪23.1.0.802067) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

... continues on next page ...

... continued from previous page ...

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)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

Vulnerability Detection Method
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`

References
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: 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`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216

... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 5.3)
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 w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D
↪626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for C
↪omplication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no su
↪ch thing outside US,C=XX (Server certificate)
```

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

Solution:
Solution type: Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

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

Vulnerability Detection Method
Checks the RSA keys size of the server certificate and all certificates in chain for a size $<$ 2048 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..`
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: `2021-12-10T12:48:00Z`

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

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

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

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
```
... continues on next page ...

... continued from previous page ...

```
↪ existing / already established SSL/TLS connection
------------------------------------------------------------------------------
↪-----------------------------------------------
TLSv1.0          | 10
```

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

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

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

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2021-11-15T10:28:20Z`

References
`cve: CVE-2011-1473`
`cve: CVE-2011-5094`
`url: https://orchilles.com/ssl-renegotiation-dos/`
`url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`url: https://www.openwall.com/lists/oss-security/2011/07/08/2`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`cert-bund: CB-K17/0980`
`cert-bund: CB-K17/0979`
`cert-bund: CB-K14/0772`
`cert-bund: CB-K13/0915`

... continues on next page ...

... continued from previous page ...

```
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
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: `SSL/TLS: Certificate Expired`

... continues on next page ...

... continued from previous page ...

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

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

Vulnerability Detection Result
'VRFY root' produces the following answer: 252 2.0.0 root

Solution:
Solution type: Workaround
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: Check if Mailserver answer to VRFY and EXPN requests
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: 2020-08-24T08:40:10Z

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

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

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

Vulnerability Detection Result
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.

... continues on next page ...

... continued from previous page ...

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 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 TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
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`

References
`cve: CVE-2015-0204`
`cve: CVE-2011-3389`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
```

... continues on next page ...

... continued from previous page ...

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: 4.3)
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: 2022-04-14T06:42:08Z

References
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936

... continues on next page ...

... continued from previous page ...

```
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-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: Certificate Signed Using A Weak Signature Algorithm

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
Signature Algorithm:  sha1WithRSAEncryption
```

Solution:
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered 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

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

References

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

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

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

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 Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2021-02-12T06:42:15Z`

References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

[return to 10.200.0.12]

2.1.20 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10

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

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.3.2

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution:
Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later.

Affected Software/OS
TWiki version prior to 4.3.2

Vulnerability Insight
Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method
Details: TWiki Cross-Site Request Forgery Vulnerability - Sep10
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: 2022-02-18T13:05:59Z

References
cve: CVE-2009-4898
url: http://www.openwall.com/lists/oss-security/2010/08/03/8
url: http://www.openwall.com/lists/oss-security/2010/08/02/17
url: http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix
url: http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is vulnerable to Cross-site Scripting (XSS) attacks.

Vulnerability Detection Result
Installed version: 1.3.2
Fixed version: 1.9.0
Installation
path / port: /mutillidae/javascript/ddsmoothmenu

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2021-06-11T08:43:18Z`

References
`cve: CVE-2012-6708`
`url: https://bugs.jquery.com/ticket/11290`
`cert-bund: WID-SEC-2022-0673`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K18/1131`
`dfn-cert: DFN-CERT-2020-0590`

Medium (CVSS: 6.1)
NVT: TWiki < 6.1.0 XSS Vulnerability

Summary
bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 6.1.0`

Solution:
Solution type: VendorFix
Update to version 6.1.0 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

TWiki version 6.0.2 and probably prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `TWiki < 6.1.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141830
Version used: `2021-08-30T08:01:20Z`

References
`cve: CVE-2018-20212`
`url: https://seclists.org/fulldisclosure/2019/Jan/7`
`url: http://twiki.org/cgi-bin/view/Codev/DownloadTWiki`

Medium (CVSS: 6.0)
NVT: TWiki Cross-Site Request Forgery Vulnerability

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

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 4.3.1`

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution:
Solution type: VendorFix
Upgrade to version 4.3.1 or later.

Affected Software/OS
TWiki version prior to 4.3.1

Vulnerability Insight
Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.

Vulnerability Detection Method
Details: `TWiki Cross-Site Request Forgery Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: `2022-02-22T15:13:46Z`

References

... continues on next page ...

... continued from previous page ...

cve: CVE-2009-1339
url: http://secunia.com/advisories/34880
url: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258
url: http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff
↪-cve-2009-1339.txt

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
The web server has the following HTTP methods enabled: TRACE

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

Solution:
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

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

Vulnerability Detection Method
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: HTTP Debugging Methods (TRACE/TRACK) Enabled
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: 2022-05-12T09:32:01Z

References
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.securityfocus.com/bid/11604
url: http://www.securityfocus.com/bid/15222
url: http://www.securityfocus.com/bid/19915
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

Medium (CVSS: 5.0)
NVT: /doc directory browsable

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

Vulnerability Detection Result
`Vulnerable URL: http://www.seclab.net/doc/`

Solution:
Solution type: Mitigation
Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:
<Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory>

Vulnerability Detection Method
Details: `/doc directory browsable`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.10056
Version used: 2022-05-12T09:32:01Z

References
cve: CVE-1999-0678
url: http://www.securityfocus.com/bid/318

Medium (CVSS: 5.0)
NVT: QWikiwiki directory traversal vulnerability

Summary
The remote host is running QWikiwiki, a Wiki application written in PHP.
The remote version of this software contains a validation input flaw which may allow an attacker to use it to read arbitrary files on the remote host with the privileges of the web server.

Vulnerability Detection Result
Vulnerable URL: http://www.seclab.net/mutillidae/index.php?page=../../../../../.
↪./../../../../../etc/passwd%00

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Vulnerability Detection Method
Details: QWikiwiki directory traversal vulnerability
OID:1.3.6.1.4.1.25623.1.0.16100
Version used: 2022-05-12T09:32:01Z

References
cve: CVE-2005-0283
url: http://www.securityfocus.com/bid/12163

Medium (CVSS: 5.0)
NVT: awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check

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

Vulnerability Detection Result
Vulnerable URL: http://www.seclab.net/mutillidae/index.php?page=/etc/passwd

... continues on next page ...

... continued from previous page ...

Impact
An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
awiki version 20100125 and prior.

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check`
OID:1.3.6.1.4.1.25623.1.0.103210
Version used: `2022-06-08T09:12:49Z`

References
`url: https://www.exploit-db.com/exploits/36047/`
`url: http://www.securityfocus.com/bid/49187`

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
```
The following input fields where identified (URL:input name):
http://www.seclab.net/dvwa/login.php:password
http://www.seclab.net/phpMyAdmin/:pma_password
http://www.seclab.net/phpMyAdmin/?D=A:pma_password
http://www.seclab.net/tikiwiki/tiki-install.php:pass
http://www.seclab.net/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

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

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2020-08-24T15:18:35Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Product detection result
`cpe:/a:apache:http_server:2.2.8`
`Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1`
`↪.0.117232)`

Summary
Apache HTTP Server is prone to a cookie information disclosure vulnerability.

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

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update to Apache HTTP Server version 2.2.22 or later.

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21.

Vulnerability Insight
The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method
Details: `Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: `2022-04-27T12:01:52Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.2.8`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2012-0053`
`url: http://secunia.com/advisories/47779`
`url: http://www.securityfocus.com/bid/51706`
`url: http://www.exploit-db.com/exploits/18442`
`url: http://rhn.redhat.com/errata/RHSA-2012-0128.html`
`url: http://httpd.apache.org/security/vulnerabilities_22.html`
`url: http://svn.apache.org/viewvc?view=revision&revision=1235454`
`url: http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html`
`cert-bund: CB-K15/0080`
`cert-bund: CB-K14/1505`
`cert-bund: CB-K14/0608`
`dfn-cert: DFN-CERT-2015-0082`
`dfn-cert: DFN-CERT-2014-1592`
`dfn-cert: DFN-CERT-2014-0635`
`dfn-cert: DFN-CERT-2013-1307`
`dfn-cert: DFN-CERT-2012-1276`
`dfn-cert: DFN-CERT-2012-1112`
`dfn-cert: DFN-CERT-2012-0928`
`dfn-cert: DFN-CERT-2012-0758`
`dfn-cert: DFN-CERT-2012-0744`
`dfn-cert: DFN-CERT-2012-0568`
`dfn-cert: DFN-CERT-2012-0425`
`dfn-cert: DFN-CERT-2012-0424`
`dfn-cert: DFN-CERT-2012-0387`

... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is vulnerable to Cross-site Scripting (XSS) attacks.

Vulnerability Detection Result
Installed version: 1.3.2
Fixed version: 1.6.3
Installation
path / port: /mutillidae/javascript/ddsmoothmenu

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later or apply the patch.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.6.3 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: 2021-06-11T09:02:34Z

References
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

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

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

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight
The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Vulnerability Detection Method
Details: `phpMyAdmin 'error.php' Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: `2022-02-18T13:05:59Z`

References
`cve: CVE-2010-4480`
`url: http://www.exploit-db.com/exploits/15699/`
`url: http://www.vupen.com/english/advisories/2010/3133`
`dfn-cert: DFN-CERT-2011-0467`
`dfn-cert: DFN-CERT-2011-0451`
`dfn-cert: DFN-CERT-2011-0016`
`dfn-cert: DFN-CERT-2011-0002`

[return to 10.200.0.12]

2.1.21 Medium 5900/tcp

Medium (CVSS: 4.8)
NVT: VNC Server Unencrypted Data Transmission

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

Vulnerability Detection Result
```
The VNC server provides the following insecure or cryptographically weak Securit
↪y Type(s):
2 (VNC authentication)
```

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

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

Vulnerability Detection Method
Details: `VNC Server Unencrypted Data Transmission`
OID:1.3.6.1.4.1.25623.1.0.108529
Version used: `2020-11-10T09:46:51Z`

References
`url: https://tools.ietf.org/html/rfc6143#page-10`

[return to 10.200.0.12]

2.1.22 Medium 2121/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

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

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt
Anonymous sessions:     331 Password required for anonymous
```

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2020-08-24T08:40:10Z`

[return to 10.200.0.12]

2.1.23 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
Vulnerability was detected according to the Vulnerability Detection Method.

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

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2022-11-18T10:11:40Z

References
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[return to 10.200.0.12]

2.1.24 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

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

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
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
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610

... continues on next page ...

... continued from previous page ...

Version used: 2021-09-20T11:05:40Z

[return to 10.200.0.12]

2.1.25 Low 5432/tcp

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.

Solution:
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ...
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2022-04-14T11:24:11Z

References
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin

... continues on next page ...

... continued from previous page ...

```
↪g-ssl-30.html
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
```

... continues on next page ...

... continued from previous page ...

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

[return to 10.200.0.12]

2.1.26 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
```

... continues on next page ...

... continued from previous page ...

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 updateto 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)
OID:1.3.6.1.4.1.25623.1.0.805188
Version used: 2022-04-14T06:42:08Z

References
cve: CVE-2015-4000
url: https://weakdh.org
url: http://www.securityfocus.com/bid/74733
url: https://weakdh.org/imperfect-forward-secrecy.pdf
url: http://openwall.com/lists/oss-security/2015/05/20/8
url: https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained
url: https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes
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

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0737

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

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.

Solution:
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2022-04-14T11:24:11Z

References
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574

... continues on next page ...

... continued from previous page ...

```
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin
↪g-ssl-30.html
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[return to 10.200.0.12]

2.1.27 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 953061
```

... continues on next page ...

... continued from previous page ...

Packet 2: 953169

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

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

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

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: TCP timestamps
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: 2020-08-24T08:40:10Z

References
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152

[return to 10.200.0.12]