

svn commit: r1887027 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml

Posted to dev@tomcat.apache.org (<list.html?dev@tomcat.apache.org>)



ma...@apache.org - Monday, March 1, 2021 6:03:56 AM EST

URL: <http://svn.apache.org/viewvc?rev=1887027&view=rev> (<http://svn.apache.org/viewvc?rev=1887027&view=rev>)
Log:
Add details for CVE-2021-25122 and CVE-2021-25329

Modified: tomcat/site/trunk/docs/security-10.html
URL: <http://svn.apache.org/viewvc/tomcat/site/trunk/docs/security-10.html?rev=1887027&r1=1887026&r2=1887027&view=diff> (<http://svn.apache.org/viewvc/tomcat/site/trunk/docs/security-10.html?rev=1887027&r1=1887026&r2=1887027&view=diff>)

[illegible]

```
+ <p>This was fixed with commit
+ <a href="https://github.com/apache/tomcat/commit/dd757c0a893e2e35f8bc1385d6967221ae8b9b9b">dd757c0a</a>.</p>
+
+ <p>This issue was identified by the Apache Tomcat Security team on 11
+ January 2021. The issue was made public on 1 March 2021.</p>
+
+ <p>Affects: 10.0.0-M1 to 10.0.0</p>
+
+</div><h3 id="Fixed_in_Apache_Tomcat_10.0.0-M10"><span class="pull-right">17 November 2020</span> Fixed in Apache Tomcat 10.0.0-M10</h3><div class="text">
+
+<p><strong>Important: Information disclosure</strong>
```

[illegible]

```
<a href="security.html">omcat Security Team</a>. Thank you.
</p>
</div><h3 id="Fixed_in_Apache_Tomcat_7.0.108"><span class="pull-right">5 February 2021</span> Fixed in Apache Tomcat 7.0.108</h3><div class="text">
<p><strong>Low: Fix for <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9484" rel="nofollow">CVE-2020-9484</a> was incomplete</strong>
<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25329" rel="nofollow">CVE-2021-25329</a></p>
<p>The fix for <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9484" rel="nofollow">CVE-2020-9484</a> was incomplete. When using a
highly unlikely configuration edge case, the Tomcat instance was still
vulnerable to <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9484" rel="nofollow">CVE-2020-9484</a>. Note that both the previously
published prerequisites for <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9484" rel="nofollow">CVE-2020-9484</a> and the previously
published non-upgrade mitigations for <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9484" rel="nofollow">CVE-2020-9484</a> also apply to
this issue.</p>
<p>This was fixed with commit
<a href="https://github.com/apache/tomcat/commit/74b105657ffbd1d1de80455f03446c3bbf30d1f5">74b10565</a>.</p>
<p>This issue was reported to the Apache Tomcat Security team by Trung Pham
of Viettel Cyber Security on 12 January 2021. The issue was made public
on 1 March 2021.</p>
<p>Affects: 7.0.0 to 7.0.107</p>
</div><h3 id="Fixed_in_Apache_Tomcat_7.0.107"><span class="pull-right">11 November 2020</span> Fixed in Apache Tomcat 7.0.107</h3><div class="text">
<p><strong>Important: Information disclosure</strong>
```

[illegible]

```

href="#Fixed_in_Apache_Tomcat_8.5.9">Fixed in Apache Tomcat 8.5.9</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.39">Fixed in Apache Tomcat 8.0.39</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.5.8">Fixed in Apache Tomcat 8.5.8</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.5.5_and_8.0.37">Fixed in Apache Tomcat 8.5.5 and 8.0.37</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.5.3_and_8.0.36">Fixed in Apache Tomcat 8.5.3 and 8.0.36</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.32">Fixed in Apache Tomcat 8.0.32</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.30">Fixed in Apache Tomcat 8.0.30</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.27">Fixed in Apache Tomcat 8.0.27</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.17">Fixed in Apache Tomcat 8.0.17</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.9">Fixed in Apache Tomcat 8.0.9</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.8">Fixed in Apache Tomcat 8.0.8</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.5">Fixed in Apache Tomcat 8.0.5</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.3">Fixed in Apache Tomcat 8.0.3</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.0-RC10">Fixed in Apache Tomcat 8.0.0-RC10</a></li><li><a href="#Fixed_in_Apache_Tomcat_8.0.0-RC3">Fixed in Apache Tomcat 8.0.0-RC3</a></li><li><a href="#Not_a_vulnerability_in_Tomcat">Not a vulnerability in Tomcat</a></li></ul>
</div><h3 id="Apache_Tomcat_8.x_vulnerabilities">Apache Tomcat 8.x vulnerabilities</h3><div class="text">
    <p>This page lists all security vulnerabilities fixed in released versions of Apache Tomcat 8.x. Each vulnerability is given a


@ -44,6 +44,9 @@


    <a href="security.html">Tomcat Security Team</a>. Thank you.
</p>
+ </div><h3 id="Fixed_in_Apache_Tomcat_8.5.63"><span class="pull-right">2 February 2021</span> Fixed in Apache Tomcat 8.5.63</h3><div class="text">
+ 
+     <p><i>Note: The issues below were fixed in Apache Tomcat 8.5.62 but the release vote for the 8.5.62 release candidate did not pass. Therefore, although users must download 8.5.63 to obtain a version that includes a fix for these issues, version 8.5.62 is not included in the list of affected versions.</i></p>
```

```

--> tomcat/site/trunk/docs/security-9.html (original)
+++ tomcat/site/trunk/docs/security-9.html Mon Mar 1 11:03:55 2021
@@ -2,7 +2,7 @@
<html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link
href=
res/css/tomcat.css" rel=
stylesheet" type=
text/css"><link href=
res/css/fonts/fonts.css" rel=
stylesheet" type=
text/css"><title>Apache Tomcat&reg; - Apache Tomcat 9
vulnerabilities</title><meta name="author" content="Apache Tomcat Project"></head><body><div id=
"wrapper"><header id=
"header"><div class=
"clearfix"><div class=
"menu-toggler pull-
left" tabindex=
"1"><div class=
"hamburger"></div></div><a href=
"http://tomcat.apache.org"><img class=
"tomcat-logo pull-left noPrint" alt=
"Tomcat Home" src=
res/images/tomcat.png"></a><h1 class=
"pull-left">Apache Tomcat<sup>®</sup></h1><div class=
"asf-logos pull-right"><a href=
"https://www.apache.org/foundation/contributing.html" target=
_blank" class=
"pull-left"><img src=
https://www.apache.org/images/Support Apache-small.png" class=
"support-asf" alt=
"Support Apache"></a><a href=
"http://www.apache.org/" target=
_blank" class=
"pull-left"><img src=
res/images/asf_logo.svg" class=
"asf-logo" alt=
"The Apache Software Foundation"></a></div></div></header><main id=
"middle"><div id=
"mainLeft"><div id=
"nav-wrapper"><form action=
https://www.google.com/search" method=
"get"><div class=
"searchbox"><input value=
"tomcat.apache.org" name=
"sitesearch" type=
"hidden"><input aria-label=
"Search text" placeholder=
"Search&hellip;" required=
"required" name=
"q" id=
"query" type=
"search"><button>Go</button></div></form><div class=
"asfevents"><a href=
https://www.apache.org/events/current-event.html"><img src=
https://www.apache.org/events/current-event-234x60.png" alt=
"Next ASF event"><br>
Save the date!
</a></div><nav><div><h2>Apache Tomcat</h2><ul><li><a href=
"/index.html">Home</li><li><a href=
"/taglibs.html">TagLibs</li><li><a href=
"/maven-plugin.html">Maven Plugin</li><li><a href=
"/div>div><h2>Download</h2><ul><li><a href=
"/whichversion.html">Which version?</li><li><a href=
https://tomcat.apache.org/download-10.cgi">Tomcat 10</li><li><a href=
https://tomcat.apache.org/download-90.cgi">Tomcat 9</li><li><a href=
https://tomcat.apache.org/download-80.cgi">Tomcat 8</li><li><a href=
https://tomcat.apache.org/download-70.cgi">Tomcat 7</li><li><a href=
https://tomcat.apache.org/download-migration.cgi">Tomcat Migration Tool for Jakarta EE</li><li><a href=
https://tomcat.apache.org/download-connectors.cgi">Tomcat Connectors</li><li><a href=
https://tomcat.apache.org/download-native.cgi">Tomcat Native</li><li><a href=
https://tomcat.apache.org/download-taglibs.cgi">TagLibs</li><li><a href=
https://archive.apache.org/dist/tomcat/">A
rchives</li><li><a href=
"/div>div><h2>Documentation</h2><ul><li><a href=
"/tomcat-10.0-doc/index.html">Tomcat 10.0</li><li><a href=
"/tomcat-9.0-doc/index.html">Tomcat 9.0</li><li><a href=
"/tomcat-8.5-doc/index.html">Tomcat 8.5</li><li><a href=
"/tomcat-7.0-doc/index.html">Tomcat 7.0</li><li><a href=
"/connectors-doc">Tomcat Connectors</li><li><a href=
"/native-doc">Tomcat Native</li><li><a href=
https://wiki.apache.org/confluence/display/TOMCAT">Wiki</li><li><a href=
"/migration.html">Migration Guides</li><li><a href=
"/presentations.html">Presentations</li><li><a href=
https://wiki.apache.org/confluence/x/B181Bg">Specifications</li><li><a href=
">Problems</li><li><a href=
"/security.html">Security Reports</li><li><a href=
"/findhelp.html">Find help</li><li><a href=
https://wiki.apache.org/confluence/display/TOMCAT/FAQ">FAQ</li><li><a href=
"/lists.html">Mailing Lists</li><li><a href=
"/bugreport.html">Bug Databases</li><li><a href=
"/irc.html">IRC</li><li><a href=
"/div>div><h2>Get Involved</h2><ul><li><a href=
"/getinvolved">Overview</li><li><a href=
"/source.html">Source code</li><li><a href=
"/ci.html">Buildbot</li><li><a href=
https://wiki.apache.org/confluence/x/vI2eZg">Translations</li><li><a href=
"/tools.html">Tools</li><li><a href=
"/div>div><h2>Media</h2><ul><li><a href=
https://twitter.com/theapachetomcat">Twitter</li><li><a href=
https://www.youtube.com/c/ApacheTomcatOfficial">YouTube</li><li><a href=
https://blogs.apache.org/tomcat/">Blogs</li><li><a href=
"/div>div><h2>Misc</h2><ul><li><a href=
"/whereare.html">Who We Are</li><li><a href=
https://www.reddubbble.com/people/comdev/works/30885254-apache-tomcat">Swag</li><li><a href=
"/heritage.html">Heritage</li><li><a href=
http://www.apache.org">Apache Home</li><li><a href=
"/resources.html">Resources</li><li><a href=
"/contact.html">Contact</li><li><a href=
"/legal.html">Legal</li><li><a href=
https://www.apache.org/foundation/contributing.html">Support Apache</li><li><a href=
https://www.apache.org/foundation/sponsorship.html">Sponsorship</li><li><a href=
http://www.apache.org/foundation/thanks.html">Thanks</li><li><a href=
http://www.apache.org/licenses/">Licenses</li><li><a href=
"/div><div><div id=
"content"><h2 style=
"display: none;">Content</h2><h3 id=
"Table_of_Contents">Table of Contents</h3><div class=
"text"><ul><li><a href=
"#Apache_Tomcat_9.x_vulnerabilities">Apache Tomcat 9.x vulnerabilities</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.40">Fixed in Apache Tomcat 9.0.40</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.38">Fixed in Apache Tomcat 9.0.38</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.37">Fixed in Apache Tomcat 9.0.37</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.36">Fixed in Apache Tomcat 9.0.36</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.35">Fixed in Apache Tomcat 9.0.35</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.34">Fixed in Apache Tomcat 9.0.34</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.33">Fixed in Apache Tomcat 9.0.33</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.32">Fixed in Apache Tomcat 9.0.32</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.31">Fixed in Apache Tomcat 9.0.31</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.30">Fixed in Apache Tomcat 9.0.30</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.29">Fixed in Apache Tomcat 9.0.29</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.28">Fixed in Apache Tomcat 9.0.28</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.27">Fixed in Apache Tomcat 9.0.27</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.26">Fixed in Apache Tomcat 9.0.26</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.25">Fixed in Apache Tomcat 9.0.25</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.24">Fixed in Apache Tomcat 9.0.24</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.23">Fixed in Apache Tomcat 9.0.23</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.22">Fixed in Apache Tomcat 9.0.22</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.21">Fixed in Apache Tomcat 9.0.21</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.20">Fixed in Apache Tomcat 9.0.20</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.19">Fixed in Apache Tomcat 9.0.19</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.18">Fixed in Apache Tomcat 9.0.18</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.17">Fixed in Apache Tomcat 9.0.17</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.16">Fixed in Apache Tomcat 9.0.16</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.15">Fixed in Apache Tomcat 9.0.15</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.14">Fixed in Apache Tomcat 9.0.14</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.13">Fixed in Apache Tomcat 9.0.13</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.12">Fixed in Apache Tomcat 9.0.12</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.11">Fixed in Apache Tomcat 9.0.11</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.10">Fixed in Apache Tomcat 9.0.10</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.9">Fixed in Apache Tomcat 9.0.9</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.8">Fixed in Apache Tomcat 9.0.8</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.7">Fixed in Apache Tomcat 9.0.7</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.6">Fixed in Apache Tomcat 9.0.6</li><li><a href=
"#Fixed_in_Apache_Tomcat_9.0.5">Fixed in Apache Tomcat 
```

```
16</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.12">Fixed in Apache Tomcat 9.0.12</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.10">Fixed in Apache Tomcat 9.0.10</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.9">Fixed in Apache Tomcat 9.0.9</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.8">Fixed in Apache Tomcat 9.0.8</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.5">Fixed in Apache Tomcat 9.0.5</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.2">Fixed in Apache Tomcat 9.0.2</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.1">Fixed in Apache Tomcat 9.0.1</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M22">Fixed in Apache Tomcat 9.0.0.M22</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M21">Fixed in Apache Tomcat 9.0.0.M21</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M19">Fixed in Apache Tomcat 9.0.0.M19</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M18">Fixed in Apache Tomcat 9.0.0.M18</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M17">Fixed in Apache Tomcat 9.0.0.M17</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M15">Fixed in Apache Tomcat 9.0.0.M15</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M13">Fixed in Apache Tomcat 9.0.0.M13</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M10">Fixed in Apache Tomcat 9.0.0.M10</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M8">Fixed in Apache Tomcat 9.0.0.M8</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M3">Fixed in Apache Tomcat 9.0.0.M3</a></li></ul>
+<ul><li><a href="#Apache_Tomcat_9.x_vulnerabilities">Apache Tomcat 9.x vulnerabilities</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.43">Fixed in Apache Tomcat 9.0.43</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.40">Fixed in Apache Tomcat 9.0.40</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.38">Fixed in Apache Tomcat 9.0.38</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.37">Fixed in Apache Tomcat 9.0.37</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.36">Fixed in Apache Tomcat 9.0.36</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.35">Fixed in Apache Tomcat 9.0.35</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.31">Fixed in Apache Tomcat 9.0.31</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.30">Fixed in Apache Tomcat 9.0.30</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.29">Fixed in Apache Tomcat 9.0.29</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.20">Fixed in Apache Tomcat 9.0.20</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.19">Fixed in Apache Tomcat 9.0.19</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.16">Fixed in Apache Tomcat 9.0.16</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.12">Fixed in Apache Tomcat 9.0.12</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.10">Fixed in Apache Tomcat 9.0.10</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.9">Fixed in Apache Tomcat 9.0.9</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.8">Fixed in Apache Tomcat 9.0.8</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.5">Fixed in Apache Tomcat 9.0.5</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.2">Fixed in Apache Tomcat 9.0.2</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.1">Fixed in Apache Tomcat 9.0.1</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M22">Fixed in Apache Tomcat 9.0.0.M22</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M21">Fixed in Apache Tomcat 9.0.0.M21</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M19">Fixed in Apache Tomcat 9.0.0.M19</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M18">Fixed in Apache Tomcat 9.0.0.M18</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M17">Fixed in Apache Tomcat 9.0.0.M17</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M15">Fixed in Apache Tomcat 9.0.0.M15</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M13">Fixed in Apache Tomcat 9.0.0.M13</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M10">Fixed in Apache Tomcat 9.0.0.M10</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M8">Fixed in Apache Tomcat 9.0.0.M8</a></li><li><a href="#Fixed_in_Apache_Tomcat_9.0.0.M3">Fixed in Apache Tomcat 9.0.0.M3</a></li></ul>
</div><h3 id="Apache_Tomcat_9.x_vulnerabilities">Apache Tomcat 9.x vulnerabilities</h3><div class="text">
  <p>This page lists all security vulnerabilities fixed in released versions of Apache Tomcat 9.x. Each vulnerability is given a
  @@ -39,6 +39,49 @@
    <a href="security.html">Tomcat Security Team</a>. Thank you.
  </p>
+
+ </div><h3 id="Fixed_in_Apache_Tomcat_9.0.43"><span class="pull-right">2 February 2021</span> Fixed in Apache Tomcat 9.0.43</h3><div class="text">
+
+ <p><i>Note: The issues below were fixed in Apache Tomcat 9.0.42 but the release vote for the 9.0.42 release candidate did not pass. Therefore, although users must download 9.0.43 to obtain a version that includes a fix for these issues, version 9.0.42 is not included in the list of affected versions.</i></p>
+
+ <p><strong>Low: Fix for <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9484" rel="nofollow">CVE-2020-9484</a> was incomplete</strong>
+ <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25329" rel="nofollow">CVE-2021-25329</a></p>
+
+ <p>The fix for <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9484" rel="nofollow">CVE-2020-9484</a> was incomplete. When using a highly unlikely configuration edge case, the Tomcat instance was still vulnerable to <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9484" rel="nofollow">CVE-2020-9484</a>. Note that both the previously published prerequisites for <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9484" rel="nofollow">CVE-2020-9484</a> and the previously published non-upgrade mitigations for <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9484" rel="nofollow">CVE-2020-9484</a> also apply to this issue.</p>
+
+ <p>This was fixed with commit
+ <a href="https://github.com/apache/tomcat/commit/d47c20a776e8919eaca8da9390a32bc8bf8210b1">d47c20a7</a>.</p>
+
+ <p>This issue was reported to the Apache Tomcat Security team by Trung Pham of Viettel Cyber Security on 12 January 2021. The issue was made public on 1 March 2021.</p>
+
+ <p>Affects: 9.0.0.M1 to 9.0.41</p>
+
+ <p><strong>Important: Request mix-up with h2c</strong>
+ <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25122" rel="nofollow">CVE-2021-25122</a></p>
+
+ <p>When responding to new h2c connection requests, Apache Tomcat could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request.</p>
+
+ <p>This was fixed with commit
+ <a href="https://github.com/apache/tomcat/commit/d47c20a776e8919eaca8da9390a32bc8bf8210b1">d47c20a7</a>.</p>
+
+ <p>This issue was identified by the Apache Tomcat Security team on 11 January 2021. The issue was made public on 1 March 2021.</p>
+
+ <p>Affects: 9.0.0.M1 to 9.0.41</p>
+
</div><h3 id="Fixed_in_Apache_Tomcat_9.0.40"><span class="pull-right">17 November 2020</span> Fixed in Apache Tomcat 9.0.40</h3><div class="text">
  <p><strong>Important: Information disclosure</strong>
```

Modified: tomcat/site/trunk/xdocs/security-10.xml

URL: http://svn.apache.org/viewvc/tomcat/site/trunk/xdocs/security-10.xml?rev=1887027&r1=1887026&r2=1887027&view=diff (http://svn.apache.org/viewvc/tomcat/site/trunk/xdocs/security-10.xml?rev=1887027&r1=1887026&r2=1887027&view=diff)

=====

```
--- tomcat/site/trunk/xdocs/security-10.xml (original)
+++ tomcat/site/trunk/xdocs/security-10.xml Mon Mar 1 11:03:55 2021
@@ -50,6 +50,51 @@

</section>

+ <section name="Fixed in Apache Tomcat 10.0.2" rtext="2 February 2021">
+
+ <p><i>Note: The issues below were fixed in Apache Tomcat 10.0.1 but the release vote for the 10.0.1 release candidate did not pass. Therefore, although users must download 10.0.2 to obtain a version that includes a fix for these issues, version 10.0.1 is not included in the list of affected versions.</i></p>
+
+ <p><strong>Low: Fix for <cve>CVE-2020-9484</cve> was incomplete</strong>
+ <cve>CVE-2021-25329</cve></p>
+
+ <p>The fix for <cve>CVE-2020-9484</cve> was incomplete. When using a highly unlikely configuration edge case, the Tomcat instance was still vulnerable to <cve>CVE-2020-9484</cve>. Note that both the previously published prerequisites for <cve>CVE-2020-9484</cve> and the previously published non-upgrade mitigations for <cve>CVE-2020-9484</cve> also apply to this issue.</p>
+
+ <p>This was fixed with commit
+ <a href="https://github.com/apache/tomcat/commit/d47c20a776e8919eaca8da9390a32bc8bf8210b1">d47c20a7</a>.</p>
```

Modified: tomcat/site/trunk/xdocs/security-7.xml
URL: http://svn.apache.org/viewvc/tomcat/site/trunk/xdocs/security-7.xml?rev=1887027&r1=1887026&r2=1887027&view=diff (http://svn.apache.org/viewvc/tomcat/site/trunk/xdocs/security-7.xml?rev=1887027&r1=1887026&r2=1887027&view=diff)

Modified: tomcat/site/trunk/xdocs/security-8.xml
URL: <http://svn.apache.org/viewvc/tomcat/site/trunk/xdocs/security-8.xml?rev=1887027&r1=1887026&r2=1887027&view=diff> (<http://svn.apache.org/viewvc/tomcat/site/trunk/xdocs/security-8.xml?rev=1887027&r1=1887026&r2=1887027&view=diff>)


```
+
+ <p>When responding to new h2c connection requests, Apache Tomcat could
+ duplicate request headers and a limited amount of request body from one
+ request to another meaning user A and user B could both see the results of
+ user A's request.</p>
+
+ <p>This was fixed with commit
+   <hashlink hash="bb0e7c1e0d737a0de7d794572517bce0e91d30fa"/>.</p>
+
+ <p>This issue was identified by the Apache Tomcat Security team on 11
+   January 2021. The issue was made public on 1 March 2021.</p>
+
+ <p>Affects: 8.5.0 to 8.5.61</p>
+
+ </section>
+
+ <section name="Fixed in Apache Tomcat 8.5.60" rtext="17 November 2020">
+
+   <p><strong>Important: Information disclosure</strong>
```

Modified: tomcat/site/trunk/xdocs/security-9.xml

URL: <http://svn.apache.org/viewvc/tomcat/site/trunk/xdocs/security-9.xml?rev=1887027&r1=1887026&r2=1887027&view=diff> (<http://svn.apache.org/viewvc/tomcat/site/trunk/xdocs/security-9.xml?rev=1887027&r1=1887026&r2=1887027&view=diff>)

```
-----
--- tomcat/site/trunk/xdocs/security-9.xml (original)
+++ tomcat/site/trunk/xdocs/security-9.xml Mon Mar  1 11:03:55 2021
@@ -50,6 +50,51 @@

</section>

+ <section name="Fixed in Apache Tomcat 9.0.43" rtext="2 February 2021">
+
+   <p><i>Note: The issues below were fixed in Apache Tomcat 9.0.42 but the
+     release vote for the 9.0.42 release candidate did not pass. Therefore,
+     although users must download 9.0.43 to obtain a version that includes a
+     fix for these issues, version 9.0.42 is not included in the list of
+     affected versions.</i></p>
+
+   <p><strong>Low: Fix for <cve>CVE-2020-9484</cve> was incomplete</strong>
+     <cve>CVE-2021-25329</cve></p>
+
+   <p>The fix for <cve>CVE-2020-9484</cve> was incomplete. When using a
+   highly unlikely configuration edge case, the Tomcat instance was still
+   vulnerable to <cve>CVE-2020-9484</cve>. Note that both the previously
+   published prerequisites for <cve>CVE-2020-9484</cve> and the previously
+   published non-upgrade mitigations for <cve>CVE-2020-9484</cve> also apply to
+   this issue.</p>
+
+   <p>This was fixed with commit
+     <hashlink hash="4785433a226a20df6acbea49296e1ce7e23de453"/>.</p>
+
+   <p>This issue was reported to the Apache Tomcat Security team by Trung Pham
+     of Viettel Cyber Security on 12 January 2021. The issue was made public
+     on 1 March 2021.</p>
+
+   <p>Affects: 9.0.0.M1 to 9.0.41</p>
+
+   <p><strong>Important: Request mix-up with h2c</strong>
+     <cve>CVE-2021-25122</cve></p>
+
+   <p>When responding to new h2c connection requests, Apache Tomcat could
+   duplicate request headers and a limited amount of request body from one
+   request to another meaning user A and user B could both see the results of
+   user A's request.</p>
+
+   <p>This was fixed with commit
+     <hashlink hash="d47c20a776e8919eaca8da9390a32bc8bf8210b1"/>.</p>
+
+   <p>This issue was identified by the Apache Tomcat Security team on 11
+     January 2021. The issue was made public on 1 March 2021.</p>
+
+   <p>Affects: 9.0.0.M1 to 9.0.41</p>
+
+ </section>
+
+ <section name="Fixed in Apache Tomcat 9.0.40" rtext="17 November 2020">
+
+   <p><strong>Important: Information disclosure</strong>
```

To unsubscribe, e-mail: dev-unsubscribe@tomcat.apache.org

For additional commands, e-mail: dev-help@tomcat.apache.org