svn commit: r1067927 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2020-13954.txt.asc security-advisories.html

Posted to commits@cxf.apache.org (list.html?commits@cxf.apache.org)

co...@apache.org - Thursday, November 12, 2020 7:31:52 AM EST

Author: coheigea
Date: Thu Nov 12 12:31:52 2020
New Revision: 1067927

Log:
Adding security advisory

Added:
websites/production/cxf/content/security-advisories.data/CVE-2020-13954.txt.asc
Modified:
websites/production/cxf/content/cache/main.pageCache
websites/production/cxf/content/security-advisories.html

Modified: websites/production/cxf/content/cache/main.pageCache
==
Binary files - no diff available.

Added: websites/production/cxf/content/security-advisories.data/CVE-2020-13954.txt.asc
==

```
--- websites/production/cxf/content/security-advisories.data/CVE-2020-13954.txt.asc (added)
+++ websites/production/cxf/content/security-advisories.data/CVE-2020-13954.txt.asc Thu Nov 12 12:31:52 2020
@@ -0,0 +1,41 @@
+-----BEGIN PGP SIGNED MESSAGE-----
+Hash: SHA512
+
+Apache CXF Reflected XSS in the services listing page via the styleSheetPath (CVE-2020-13954)
+
+PRODUCT AFFECTED:
+
+This issue affects Apache CXF.
+
+PROBLEM:
+
+By default, Apache CXF creates a /services page containing a listing of the available endpoint names and addresses. This webpage is vulnerable to a reflected Cross-Site Scripting
(XSS) attack via the styleSheetPath, which allows a malicious actor to inject javascript into the web page.
+
+This vulnerability affects all versions of Apache CXF prior to 3.4.1 and 3.3.8.
+
+Please note that this is a separate issue to CVE-2019-17573.
+
+This issue has been assigned CVE-2020-13954.
+
+WORKAROUND:
+
+Users of Apache CXF should update to either 3.3.8 or 3.4.1. Alternatively, it is possible to disable the service listing altogether by setting the "hide-service-list-page" servlet
parameter to "true".
+
+RELATED LINKS:
+
+CVE-2020-13954 at cve.mitre.org
+
+ACKNOWLEDGEMENTS:
+
+Thanks to Ryan Lambeth for reporting this issue.
+-----BEGIN PGP SIGNATURE-----
+
+iQEzBAEBCgAdFiEE20Xs0ZuXUU9ycQWuZ7+AsQrVOYMFAl+tKGUACgkQZ7+AsQrV
+OYOejAf/YSmg5GoWhWB77V5P21yHigEus1Zgg68iNJ9tm6QXEJafJ0UEibPaFKpO
+4N4UyBa4ur7ULbRQuzxL+wru5DkhDaKKdmEvSv9MHrqOGqy2Zz6m3154+3VgMuB7
+DS7eGqDe4LihkmdI4qubWw45etdX3POAcU9tIDNsfnBX9b4zuvNYbrezDPbk+irM
+BfmTl9MO1D/D3W5qetpCHDCtQYtJ/yKC0C9yri8tna8FwL30Jpu+w34H+hNYOQRw
+2Kud/r/tm5crFsdCCqealNSoUtxg/BvLCu8owLODjHt6acf6axuPA36EPzl/7+fH
+VD8jsCX0FeSsagBefJDQyNkj5BKgSg==
+=3le2
+-----END PGP SIGNATURE-----
```

Modified: websites/production/cxf/content/security-advisories.html
==

```
--- websites/production/cxf/content/security-advisories.html (original)
+++ websites/production/cxf/content/security-advisories.html Thu Nov 12 12:31:52 2020
@@ -99,7 +99,7 @@ Apache CXF -- Security Advisories
          <td height="100%">
            <!-- Content -->
            <div class="wiki-content">
-<div id="ConfluenceContent"><h3 id="SecurityAdvisories-2020">2020</h3><ul><li><a shape="rect" href="security-advisories.data/CVE-2020-1954.txt.asc?
version=1&amp;modificationDate=1585730169000&amp;api=v2" data-linked-resource-id="148645097" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2020-1954.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="37">CVE-2020-1954</a>: Apache CXF JMX Integration is vulnerable to a MITM attack</li></ul><h3 id="SecurityAdvisories-2019">2019</h3><ul><li><a
shape="rect" href="security-advisories.data/CVE-2019-17573.txt.asc?version=2&amp;modificationDate=1584610519000&amp;api=v2" data-linked-resource-id="145722246" data-linked-resource-
version="2" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2019-17573.txt.asc" data-nice-type="Text File" data-
 linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2019-17573</a>: Apache CXF Reflected XSS in
the services listing page</li><li><a shape="rect" href="security-advisories.data/CVE-2019-12423.txt.asc?version=1&amp;modificationDate=1579178393000&amp;api=v2" data-linked-
resource-id="145722244" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2019-12423.txt.asc" data-nice-type="Text
File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2019-12423</a>: Apache CXF OpenId
Connect JWK Keys service returns private/secret credentials if configured with a jwk keystore</li><li><a shape="rect" href="security-advisories.data/CVE-2019-12419.txt.asc?
version=2&amp;modificationDate=1572961201000&amp;api=v2" data-linked-resource-id="135859612" data-linked-resource-ve
 rsion="2" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2019-12419.txt.asc" data-nice-type="Text File" data-linked-resource-content-
type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2019-12419</a>: Apache CXF OpenId Connect token service does not
properly validate the clientId</li><li><a shape="rect" href="security-advisories.data/CVE-2019-12406.txt.asc?version=1&amp;modificationDate=1572957147000&amp;api=v2" data-linked-
resource-id="135859607" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2019-12406.txt.asc" data-nice-type="Text
File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2019-12406</a>: Apache CXF does not
restrict the number of message attachments</li></ul><h3 id="SecurityAdvisories-2018">2018</h3><ul><li><a shape="rect" h
 ref="security-advisories.data/CVE-2018-8039.txt.asc?version=1&amp;modificationDate=1530184663000&amp;api=v2" data-linked-resource-id="87296645" data-linked-resource-version="1"
data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2018-8039.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-
linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2018-8039</a>: Apache CXF TLS hostname verification does not work correctly with
com.sun.net.ssl.</li><li><a shape="rect" href="security-advisories.data/CVE-2018-8038.txt.asc?version=1&amp;modificationDate=1530712328000&amp;api=v2" data-linked-resource-
id="87297524" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2018-8038.txt.asc" data-nice-type="Text File" data-
linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version
 ="37">CVE-2018-8038</a>: Apache CXF Fediz is vulnerable to DTD based XML attacks</li></ul><h3 id="SecurityAdvisories-2017">2017</h3><ul><li><a shape="rect" href="security-
advisories.data/CVE-2017-12631.txt.asc?version=1&amp;modificationDate=1512037276000&amp;api=v2" data-linked-resource-id="74688816" data-linked-resource-version="1" data-linked-
resource-type="attachment" data-linked-resource-default-alias="CVE-2017-12631.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-
resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2017-12631</a>: CSRF vulnerabilities in the Apache CXF Fediz Spring plugins.</li><li><a shape="rect"
href="security-advisories.data/CVE-2017-12624.txt.asc?version=1&amp;modificationDate=1510661632000&amp;api=v2" data-linked-resource-id="74687100" data-linked-resource-version="1"
data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2017-12624.txt.asc" data-nice-type="T
 ext File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2017-12624</a>: Apache CXF web
services that process attachments are vulnerable to Denial of Service (DoS) attacks.</li><li><a shape="rect" href="security-advisories.data/CVE-2017-7662.txt.asc?
```

```
version=1&amp;modificationDate=1494949377000&amp;api=v2" data-linked-resource-id="70255583" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2017-7662.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="37">CVE-2017-7662</a>: The Apache CXF Fediz OIDC Client Registration Service is vulnerable to CSRF attacks.</li><li><a shape="rect" href="security-
advisories.data/CVE-2017-7661.txt.asc?version=1&amp;modificationDate=1494949364000&amp;api=v2" data-linked-resource-id="70255
 582" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2017-7661.txt.asc" data-nice-type="Text File" data-linked-
resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2017-7661</a>: The Apache CXF Fediz Jetty and Spring
plugins are vulnerable to CSRF attacks.</li><li><a shape="rect" href="security-advisories.data/CVE-2017-5656.txt.asc?version=1&amp;modificationDate=1492515113000&amp;api=v2" data-
linked-resource-id="69406543" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2017-5656.txt.asc" data-nice-type="Text
File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2017-5656</a>: Apache CXF's
STSClient uses a flawed way of caching tokens that are associated with delegation tokens.</li><li><a shape
 ="rect" href="security-advisories.data/CVE-2017-5653.txt.asc?version=1&amp;modificationDate=1492515074000&amp;api=v2" data-linked-resource-id="69406542" data-linked-resource-
version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2017-5653.txt.asc" data-nice-type="Text File" data-linked-resource-content-
type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2017-5653</a>: Apache CXF JAX-RS XML Security streaming clients do not
validate that the service response was signed or encrypted.</li><li><a shape="rect" href="security-advisories.data/CVE-2017-3156.txt.asc?
version=1&amp;modificationDate=1487590374000&amp;api=v2" data-linked-resource-id="68715428" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2017-3156.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="278375
 02" data-linked-resource-container-version="37">CVE-2017-3156</a>: Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks</li></ul><h3
id="SecurityAdvisories-2016">2016</h3><ul><li><a shape="rect" href="security-advisories.data/CVE-2016-8739.txt.asc?version=1&amp;modificationDate=1482164360000&amp;api=v2" data-
linked-resource-id="67635454" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2016-8739.txt.asc" data-nice-type="Text
File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2016-8739</a>: Atom entity provider
of Apache CXF JAX-RS is vulnerable to XXE</li><li><a shape="rect" href="security-advisories.data/CVE-2016-6812.txt.asc?version=1&amp;modificationDate=1482164360000&amp;api=v2" data-
linked-resource-id="67635455" data-linked-resource-version="1" data-linked-resource-type="attachment" data-
 linked-resource-default-alias="CVE-2016-6812.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-
linked-resource-container-version="37">CVE-2016-6812</a>: XSS risk in Apache CXF FormattedServiceListWriter when a request URL contains matrix parameters</li><li><a shape="rect"
href="security-advisories.data/CVE-2016-4464.txt.asc?version=1&amp;modificationDate=1473350153000&amp;api=v2" data-linked-resource-id="65869472" data-linked-resource-version="1"
data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2016-4464.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-
linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2016-4464</a>: Apache CXF Fediz application plugins do not match the SAML AudienceRestriction
values against the list of configured audience URIs</li></ul><h3 id="SecurityAdvisories-2015">2015</h3><
 ul><li><a shape="rect" href="security-advisories.data/CVE-2015-5253.txt.asc?version=1&amp;modificationDate=1447433340000&amp;api=v2" data-linked-resource-id="61328642" data-linked-
resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2015-5253.txt.asc" data-nice-type="Text File" data-linked-resource-content-
type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2015-5253</a>: Apache CXF SAML SSO processing is vulnerable to a
wrapping attack</li><li><a shape="rect" href="security-advisories.data/CVE-2015-5175.txt.asc?version=1&amp;modificationDate=1440598018000&amp;api=v2" data-linked-resource-
id="61316328" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2015-5175.txt.asc" data-nice-type="Text File" data-
linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-
 version="37">CVE-2015-5175</a>: Apache CXF Fediz application plugins are vulnerable to Denial of Service (DoS) attacks</li></ul><h3 id="SecurityAdvisories-2014">2014</h3><ul><li><a
shape="rect" href="security-advisories.data/CVE-2014-3577.txt.asc?version=1&amp;modificationDate=1419245371000&amp;api=v2" data-linked-resource-id="51183657" data-linked-resource-
version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-3577.txt.asc" data-nice-type="Text File" data-linked-resource-content-
type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2014-3577</a>: Apache CXF SSL hostname verification bypass</li><li><a
shape="rect" href="security-advisories.data/CVE-2014-3566.txt.asc?version=1&amp;modificationDate=1418740474000&amp;api=v2" data-linked-resource-id="50561078" data-linked-resource-
version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-3566.txt.asc" d
 ata-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">Note on CVE-2014-
3566</a>: SSL 3.0 support in Apache CXF, aka the "POODLE" attack.</li><li><a shape="rect" href="security-advisories.data/CVE-2014-3623.txt.asc?
version=1&amp;modificationDate=1414169368000&amp;api=v2" data-linked-resource-id="47743195" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2014-3623.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="37">CVE-2014-3623</a>: Apache CXF does not properly enforce the security semantics of SAML SubjectConfirmation methods when used with the
TransportBinding</li><li><a shape="rect" href="security-advisories.data/CVE-2014-3584.txt.asc?version=1&amp;modificationDate=1414169326000&amp;api=v2" data
 -linked-resource-id="47743194" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-3584.txt.asc" data-nice-
type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2014-3584</a>: Apache
CXF JAX-RS SAML handling is vulnerable to a Denial of Service (DoS) attack</li><li><a shape="rect" href="security-advisories.data/CVE-2014-0109.txt.asc?
version=1&amp;modificationDate=1398873370000&amp;api=v2" data-linked-resource-id="40895138" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2014-0109.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="37">CVE-2014-0109</a>: HTML content posted to SOAP endpoint could cause OOM errors</li><li><a shape="rect" href=
 "security-advisories.data/CVE-2014-0110.txt.asc?version=1&amp;modificationDate=1398873378000&amp;api=v2" data-linked-resource-id="40895139" data-linked-resource-version="1" data-
linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-0110.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-
resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2014-0110</a>: Large invalid content could cause temporary space to fill</li><li><a shape="rect"
href="security-advisories.data/CVE-2014-0034.txt.asc?version=1&amp;modificationDate=1398873385000&amp;api=v2" data-linked-resource-id="40895140" data-linked-resource-version="1"
data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-0034.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-
linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2014-0034</a>: The
 SecurityTokenService accepts certain invalid SAML Tokens as valid</li><li><a shape="rect" href="security-advisories.data/CVE-2014-0035.txt.asc?
version=1&amp;modificationDate=1398873391000&amp;api=v2" data-linked-resource-id="40895141" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2014-0035.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="37">CVE-2014-0035</a>: UsernameTokens are sent in plaintext with a Symmetric EncryptBeforeSigning policy</li></ul><h3 id="SecurityAdvisories-
2013">2013</h3><ul><li><a shape="rect" href="security-advisories.data/CVE-2013-2160.txt.asc?version=1&amp;modificationDate=1372324301000&amp;api=v2" data-linked-resource-
id="33095710" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2013-2160.txt.asc" data-nice-type="
 Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="37">CVE-2013-2160</a> - Denial of
Service Attacks on Apache CXF</li><li><a shape="rect" href="cve-2012-5575.html">Note on CVE-2012-5575</a> - XML Encryption backwards compatibility attack on Apache CXF.</li><li><a
shape="rect" href="cve-2013-0239.html">CVE-2013-0239</a> - Authentication bypass in the case of WS-SecurityPolicy enabled plaintext UsernameTokens.</li></ul><h3
id="SecurityAdvisories-2012">2012</h3><ul><li><a shape="rect" href="cve-2012-5633.html">CVE-2012-5633</a> - WSS4JInInterceptor always allows HTTP Get requests from browser.</li><li>
<a shape="rect" href="note-on-cve-2011-2487.html">Note on CVE-2011-2487</a> - Bleichenbacher attack against distributed symmetric key in WS-Security.</li><li><a shape="rect"
href="cve-2012-3451.html">CVE-2012-3451</a> - Apache CXF is vulnerable to SOAP Action spoofing attacks on Document Literal w
 eb services.</li><li><a shape="rect" href="cve-2012-2379.html">CVE-2012-2379</a> - Apache CXF does not verify that elements were signed or encrypted by a particular Supporting
Token.</li><li><a shape="rect" href="cve-2012-2378.html">CVE-2012-2378</a> - Apache CXF does not pick up some child policies of WS-SecurityPolicy 1.1 SupportingToken policy
assertions on the client side.</li><li><a shape="rect" href="note-on-cve-2011-1096.html">Note on CVE-2011-1096</a> - XML Encryption flaw / Character pattern encoding attack.</li>
<li><a shape="rect" href="cve-2012-0803.html">CVE-2012-0803</a> - Apache CXF does not validate UsernameToken policies correctly.</li></ul><h3 id="SecurityAdvisories-2010">2010</h3>
<ul><li><a shape="rect" class="external-link" href="http://svn.apache.org/repos/asf/cxf/trunk/security/CVE-2010-2076.pdf">CVE-2010-2076</a> - DTD based XML attacks.</li></ul></div>
+<div id="ConfluenceContent"><h3 id="SecurityAdvisories-2020">2020</h3><ul><li><a shape="rect" href="security-advisories.data/CVE-2020-13954.txt.asc?
version=1&amp;modificationDate=1605183670659&amp;api=v2" data-linked-resource-id="165225095" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2020-13954.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="38">CVE-2020-13954</a>: Apache CXF Reflected XSS in the services listing page via the styleSheetPath</li><li><a shape="rect" href="security-
advisories.data/CVE-2020-1954.txt.asc?version=1&amp;modificationDate=1585730169000&amp;api=v2" data-linked-resource-id="148645097" data-linked-resource-version="1" data-linked-
resource-type="attachment" data-linked-resource-default-alias="CVE-2020-1954.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="t
 ext/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="38">CVE-2020-1954</a>: Apache CXF JMX Integration is vulnerable to a MITM
attack</li></ul><h3 id="SecurityAdvisories-2019">2019</h3><ul><li><a shape="rect" href="security-advisories.data/CVE-2019-17573.txt.asc?
version=2&amp;modificationDate=1584610519000&amp;api=v2" data-linked-resource-id="145722246" data-linked-resource-version="2" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2019-17573.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="38">CVE-2019-17573</a>: Apache CXF Reflected XSS in the services listing page</li><li><a shape="rect" href="security-advisories.data/CVE-2019-
12423.txt.asc?version=1&amp;modificationDate=1579178393000&amp;api=v2" data-linked-resource-id="145722244" data-linked-resource-version="1" data-linked-resource-type
 ="attachment" data-linked-resource-default-alias="CVE-2019-12423.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-
id="27837502" data-linked-resource-container-version="38">CVE-2019-12423</a>: Apache CXF OpenId Connect JWK Keys service returns private/secret credentials if configured with a jwk
keystore</li><li><a shape="rect" href="security-advisories.data/CVE-2019-12419.txt.asc?version=2&amp;modificationDate=1572961201000&amp;api=v2" data-linked-resource-id="135859612"
data-linked-resource-version="2" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2019-12419.txt.asc" data-nice-type="Text File" data-linked-resource-
content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="38">CVE-2019-12419</a>: Apache CXF OpenId Connect token service does
not properly validate the clientId</li><li><a shape="rect" href="security-advisories.data/CVE-201
 9-12406.txt.asc?version=1&amp;modificationDate=1572957147000&amp;api=v2" data-linked-resource-id="135859607" data-linked-resource-version="1" data-linked-resource-type="attachment"
data-linked-resource-default-alias="CVE-2019-12406.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502"
data-linked-resource-container-version="38">CVE-2019-12406</a>: Apache CXF does not restrict the number of message attachments</li></ul><h3 id="SecurityAdvisories-2018">2018</h3>
<ul><li><a shape="rect" href="security-advisories.data/CVE-2018-8039.txt.asc?version=1&amp;modificationDate=1530184663000&amp;api=v2" data-linked-resource-id="87296645" data-linked-
resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2018-8039.txt.asc" data-nice-type="Text File" data-linked-resource-content-
type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="
 38">CVE-2018-8039</a>: Apache CXF TLS hostname verification does not work correctly with com.sun.net.ssl.</li><li><a shape="rect" href="security-advisories.data/CVE-2018-
8038.txt.asc?version=1&amp;modificationDate=1530712328000&amp;api=v2" data-linked-resource-id="87297524" data-linked-resource-version="1" data-linked-resource-type="attachment"
data-linked-resource-default-alias="CVE-2018-8038.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502"
data-linked-resource-container-version="38">CVE-2018-8038</a>: Apache CXF Fediz is vulnerable to DTD based XML attacks</li></ul><h3 id="SecurityAdvisories-2017">2017</h3><ul><li><a
shape="rect" href="security-advisories.data/CVE-2017-12631.txt.asc?version=1&amp;modificationDate=1512037276000&amp;api=v2" data-linked-resource-id="74688816" data-linked-resource-
version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2017-12631.txt.asc"
 data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="38">CVE-2017-
12631</a>: CSRF vulnerabilities in the Apache CXF Fediz Spring plugins.</li><li><a shape="rect" href="security-advisories.data/CVE-2017-12624.txt.asc?
version=1&amp;modificationDate=1510661632000&amp;api=v2" data-linked-resource-id="74687100" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2017-12624.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="38">CVE-2017-12624</a>: Apache CXF web services that process attachments are vulnerable to Denial of Service (DoS) attacks.</li><li><a shape="rect"
```

```
href="security-advisories.data/CVE-2017-7662.txt.asc?version=1&amp;modificationDate=1494949377000&amp;api=v2" data-linked-resource-id="70255583"
  data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2017-7662.txt.asc" data-nice-type="Text File" data-linked-resource-
content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="38">CVE-2017-7662</a>: The Apache CXF Fediz OIDC Client Registration
Service is vulnerable to CSRF attacks.</li><li><a shape="rect" href="security-advisories.data/CVE-2017-7661.txt.asc?version=1&amp;modificationDate=1494949364000&amp;api=v2" data-
linked-resource-id="70255582" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2017-7661.txt.asc" data-nice-type="Text
File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="38">CVE-2017-7661</a>: The Apache CXF Fediz
Jetty and Spring plugins are vulnerable to CSRF attacks.</li><li><a shape="rect" href="security
 -advisories.data/CVE-2017-5656.txt.asc?version=1&amp;modificationDate=1492515113000&amp;api=v2" data-linked-resource-id="69406543" data-linked-resource-version="1" data-linked-
resource-type="attachment" data-linked-resource-default-alias="CVE-2017-5656.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-
container-id="27837502" data-linked-resource-container-version="38">CVE-2017-5656</a>: Apache CXF's STSClient uses a flawed way of caching tokens that are associated with delegation
tokens.</li><li><a shape="rect" href="security-advisories.data/CVE-2017-5653.txt.asc?version=1&amp;modificationDate=1492515074000&amp;api=v2" data-linked-resource-id="69406542"
data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2017-5653.txt.asc" data-nice-type="Text File" data-linked-resource-
content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-
 version="38">CVE-2017-5653</a>: Apache CXF JAX-RS XML Security streaming clients do not validate that the service response was signed or encrypted.</li><li><a shape="rect"
href="security-advisories.data/CVE-2017-3156.txt.asc?version=1&amp;modificationDate=1487590374000&amp;api=v2" data-linked-resource-id="68715428" data-linked-resource-version="1"
data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2017-3156.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-
linked-resource-container-id="27837502" data-linked-resource-container-version="38">CVE-2017-3156</a>: Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the
timing attacks</li></ul><h3 id="SecurityAdvisories-2016">2016</h3><ul><li><a shape="rect" href="security-advisories.data/CVE-2016-8739.txt.asc?
version=1&amp;modificationDate=1482164360000&amp;api=v2" data-linked-resource-id="67635454" data-linked-resource-version="1" data-linked-resource-type=
 "attachment" data-linked-resource-default-alias="CVE-2016-8739.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-
id="27837502" data-linked-resource-container-version="38">CVE-2016-8739</a>: Atom entity provider of Apache CXF JAX-RS is vulnerable to XXE</li><li><a shape="rect" href="security-
advisories.data/CVE-2016-6812.txt.asc?version=1&amp;modificationDate=1482164360000&amp;api=v2" data-linked-resource-id="67635455" data-linked-resource-version="1" data-linked-
resource-type="attachment" data-linked-resource-default-alias="CVE-2016-6812.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-
container-id="27837502" data-linked-resource-container-version="38">CVE-2016-6812</a>: XSS risk in Apache CXF FormattedServiceListWriter when a request URL contains matrix
parameters</li><li><a shape="rect" href="security-advisories.data/CVE-2016-4464.txt.asc?version=1&amp;modificatio
 nDate=1473350153000&amp;api=v2" data-linked-resource-id="65869472" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-
2016-4464.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-
version="38">CVE-2016-4464</a>: Apache CXF Fediz application plugins do not match the SAML AudienceRestriction values against the list of configured audience URIs</li></ul><h3
id="SecurityAdvisories-2015">2015</h3><ul><li><a shape="rect" href="security-advisories.data/CVE-2015-5253.txt.asc?version=1&amp;modificationDate=1447433340000&amp;api=v2" data-
linked-resource-id="61328642" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2015-5253.txt.asc" data-nice-type="Text
File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-reso
 urce-container-version="38">CVE-2015-5253</a>: Apache CXF SAML SSO processing is vulnerable to a wrapping attack</li><li><a shape="rect" href="security-advisories.data/CVE-2015-
5175.txt.asc?version=1&amp;modificationDate=1440598018000&amp;api=v2" data-linked-resource-id="61316328" data-linked-resource-version="1" data-linked-resource-type="attachment"
data-linked-resource-default-alias="CVE-2015-5175.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502"
data-linked-resource-container-version="38">CVE-2015-5175</a>: Apache CXF Fediz application plugins are vulnerable to Denial of Service (DoS) attacks</li></ul><h3
id="SecurityAdvisories-2014">2014</h3><ul><li><a shape="rect" href="security-advisories.data/CVE-2014-3577.txt.asc?version=1&amp;modificationDate=1419245371000&amp;api=v2" data-
linked-resource-id="51183657" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-de
 fault-alias="CVE-2014-3577.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-
container-version="38">CVE-2014-3577</a>: Apache CXF SSL hostname verification bypass</li><li><a shape="rect" href="security-advisories.data/CVE-2014-3566.txt.asc?
version=1&amp;modificationDate=1418740474000&amp;api=v2" data-linked-resource-id="50561078" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2014-3566.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="38">Note on CVE-2014-3566</a>: SSL 3.0 support in Apache CXF, aka the "POODLE" attack.</li><li><a shape="rect" href="security-advisories.data/CVE-2014-
3623.txt.asc?version=1&amp;modificationDate=1414169368000&amp;api=v2" data-linked-resource-id="47743195" data-linked-resource
 -version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-3623.txt.asc" data-nice-type="Text File" data-linked-resource-content-
type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="38">CVE-2014-3623</a>: Apache CXF does not properly enforce the security
semantics of SAML SubjectConfirmation methods when used with the TransportBinding</li><li><a shape="rect" href="security-advisories.data/CVE-2014-3584.txt.asc?
version=1&amp;modificationDate=1414169326000&amp;api=v2" data-linked-resource-id="47743194" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2014-3584.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="38">CVE-2014-3584</a>: Apache CXF JAX-RS SAML handling is vulnerable to a Denial of Service (DoS) attack</li><li>
 <a shape="rect" href="security-advisories.data/CVE-2014-0109.txt.asc?version=1&amp;modificationDate=1398873370000&amp;api=v2" data-linked-resource-id="40895138" data-linked-
resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-0109.txt.asc" data-nice-type="Text File" data-linked-resource-content-
type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="38">CVE-2014-0109</a>: HTML content posted to SOAP endpoint could cause OOM
errors</li><li><a shape="rect" href="security-advisories.data/CVE-2014-0110.txt.asc?version=1&amp;modificationDate=1398873378000&amp;api=v2" data-linked-resource-id="40895139" data-
linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-0110.txt.asc" data-nice-type="Text File" data-linked-resource-
content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="38">
 CVE-2014-0110</a>: Large invalid content could cause temporary space to fill</li><li><a shape="rect" href="security-advisories.data/CVE-2014-0034.txt.asc?
version=1&amp;modificationDate=1398873385000&amp;api=v2" data-linked-resource-id="40895140" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2014-0034.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="38">CVE-2014-0034</a>: The SecurityTokenService accepts certain invalid SAML Tokens as valid</li><li><a shape="rect" href="security-advisories.data/CVE-
2014-0035.txt.asc?version=1&amp;modificationDate=1398873391000&amp;api=v2" data-linked-resource-id="40895141" data-linked-resource-version="1" data-linked-resource-type="attachment"
data-linked-resource-default-alias="CVE-2014-0035.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/p
 lain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="38">CVE-2014-0035</a>: UsernameTokens are sent in plaintext with a Symmetric
EncryptBeforeSigning policy</li></ul><h3 id="SecurityAdvisories-2013">2013</h3><ul><li><a shape="rect" href="security-advisories.data/CVE-2013-2160.txt.asc?
version=1&amp;modificationDate=1372324301000&amp;api=v2" data-linked-resource-id="33095710" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-default-alias="CVE-2013-2160.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="38">CVE-2013-2160</a> - Denial of Service Attacks on Apache CXF</li><li><a shape="rect" href="cve-2012-5575.html">Note on CVE-2012-5575</a> - XML
Encryption backwards compatibility attack on Apache CXF.</li><li><a shape="rect" href="cve-2013-0239.html">CVE-2013-0239</a> - Authentication byp
 ass in the case of WS-SecurityPolicy enabled plaintext UsernameTokens.</li></ul><h3 id="SecurityAdvisories-2012">2012</h3><ul><li><a shape="rect" href="cve-2012-5633.html">CVE-
2012-5633</a> - WSS4JInInterceptor always allows HTTP Get requests from browser.</li><li><a shape="rect" href="note-on-cve-2011-2487.html">Note on CVE-2011-2487</a> - Bleichenbacher
attack against distributed symmetric key in WS-Security.</li><li><a shape="rect" href="cve-2012-3451.html">CVE-2012-3451</a> - Apache CXF is vulnerable to SOAP Action spoofing
attacks on Document Literal web services.</li><li><a shape="rect" href="cve-2012-2379.html">CVE-2012-2379</a> - Apache CXF does not verify that elements were signed or encrypted by
a particular Supporting Token.</li><li><a shape="rect" href="cve-2012-2378.html">CVE-2012-2378</a> - Apache CXF does not pick up some child policies of WS-SecurityPolicy 1.1
SupportingToken policy assertions on the client side.</li><li><a shape="rect" href="note-on-cve-2011-1096.ht
 ml">Note on CVE-2011-1096</a> - XML Encryption flaw / Character pattern encoding attack.</li><li><a shape="rect" href="cve-2012-0803.html">CVE-2012-0803</a> - Apache CXF does not
validate UsernameToken policies correctly.</li></ul><h3 id="SecurityAdvisories-2010">2010</h3><ul><li><a shape="rect" class="external-link"
href="http://svn.apache.org/repos/asf/cxf/trunk/security/CVE-2010-2076.pdf">CVE-2010-2076</a> - DTD based XML attacks.</li></ul></div>
            </div>
            <!-- Content -->
          </td>
```