

svn commit: r1073270 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2021-22696.txt.asc security-advisories.html

Posted to [commits@cxf.apache.org](mailto:commits@cxf.apache.org) ([list.html?commits@cxf.apache.org](http://list.html?commits@cxf.apache.org))



co...@apache.org - Friday, April 2, 2021 5:46:11 AM EDT

Log:  
Adding security advisory

Modified: websites/production/cxf/content/cache/main.pageCache

Binary files - no diff available.

Added: websites/production/cxf/content/security-advisories.data/CVE-2021-22696.txt.asc

```

-- websites/production/cxf/content/security-advisories.data/CVE-2021-22696.txt.asc (added)
+++ websites/production/cxf/content/security-advisories.data/CVE-2021-22696.txt.asc Fri Apr 2 09:46:11 2021
@@ -0,0 +1,31 @@
+-----BEGIN PGP SIGNED MESSAGE-----
+Hash: SHA512
+
++0Auth 2 authorization service vulnerable to DDos attacks (CVE-2021-22696)
+
++PRODUCT AFFECTED:
+
++This issue affects Apache CXF.
+
++PROBLEM:
+
++CXF supports (via JwtRequestCodeFilter) passing OAuth 2 parameters via a JWT token as opposed to query parameters (see: The OAuth 2.0 Authorization Framework: JWT Secured
Authorization Request (JAR)). Instead of sending a JWT token as a "request" parameter, the spec also supports specifying a URI from which to retrieve a JWT token from via the
"request_uri" parameter.
+
++CXF was not validating the "request_uri" parameter (apart from ensuring it uses "https") and was making a REST request to the parameter in the request to retrieve a token.
+
++This means that CXF was vulnerable to DDos attacks on the authorization server, as specified in section 10.4.1 of the spec.
+
++This issue affects Apache CXF versions prior to 3.4.3; Apache CXF versions prior to 3.3.10.
+
++This issue has been assigned CVE-2021-22696.
+-----BEGIN PGP SIGNATURE-----
+
+iQEzBAEBGAdFIEE20xs0ZuXu9ycQWuZ7+AsQrVOYMFAMbm444ACgkQZ7+AsQrV
+0YMP8AF+LkmoCnKzWkWiXphdIGrefAvKJNhpBu6msBs8BRU+4kwGV5jjSaHpg
+1sYeDdxV1qQzWiRLXluyDIwLd+1Y6FEYurC5ZAi9Mhd1M0B+1iFF1asxmVK+4Iyg
++NphtgDCFGAM0D6VFR5LDX0Ib6E1mM+gTKpLKMy7NUJUw4mDRAAmQvrpKzsnI/
++OE+zVFL8crotUQiDN0jclUncaZt/i+P3jNft5/77YrQmWgYcmuDTp5MzDTRPUjaF
++svj/kI8x+Uj2eZBRqUUYnJJMy2tmLKWw47d9/cGqJZ00qip/caFntDYsFECt13Z3
++bU+bEzRGdbEiTRS3mj1bSvwzK+RxZg==
+=R17L
+-----END PGP SIGNATURE-----

```

Modified: [websites/production/cxf/content/security-advisories.html](https://websites/production/cxf/content/security-advisories.html)

```

websites/production/cxf/content/security-advisories.html (original)
+++ websites/production/cxf/content/security-advisories.html Fri Apr 2 09:46:11 2021
@@ -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-2020-13954.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=1585730169900&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 Sorin plugins are vulnerable to CSRF attacks.</li><li><a shape="rect" href="security

```

```
c" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="39">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="39">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="39">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="39">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="39">CVE-2017-7661</a>; The Apache CXF Fediz Jetty and Spring plugins are vulnerable to CSRF attacks.</li></ul>
```

version=1&api=1&modificationDate=1492515113000&api=v2" data-linked-resource-id="69406543" 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="39">CVE-2017-3156</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" 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="39">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&modificationDate=1487590374000&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="39">CVE-2017-3156</a>: Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks</li><li><a shape="rect" href="security-advisories.data/CVE-2016-8739.txt.asc?version=1&modificationDate=1482164360000&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="39">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&modificationDate=1482164360000&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="39">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&modificationDate=1473350153000&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="39">CVE-2016-4464</a>: Apache CXF Fediz application plugins do not match the SAML AudienceRestriction values against the list of configured audience URIs</li><li><a shape="rect" href="security-advisories.data/CVE-2015-5253.txt.asc?version=1&modificationDate=1447433340000&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="39">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&modificationDate=1440598018000&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="39">CVE-2015-5175</a>: Apache CXF Fediz application plugins are vulnerable to Denial of Service (DoS) attacks</li><li><a shape="rect" href="security-advisories.data/CVE-2014-3577.txt.asc?version=1&modificationDate=1419245371000&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="39">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&modificationDate=1418740474000&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="39">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&modificationDate=1414169368000&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="39">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&modificationDate=1414169326000&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="39">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&modificationDate=1398873370000&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="39">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&modificationDate=1398873378000&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="39">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&modificationDate=1398873385000&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="39">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&modificationDate=1398873391000&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="39">CVE-2014-0035</a>: UsernameTokens are sent in plaintext with a Symmetric EncryptBeforeSigning policy</li><li><a shape="rect" href="security-advisories.data/CVE-2013-2160.txt.asc?version=1&modificationDate=1372324301000&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="39">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><li><a shape="rect" href="security-advisories.data/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 WSS4JInInterceptor always allows HTTP Get requests from browser.</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><li><a shape="rect" href="SecurityAdvisories-2010">2010</a><li><a shape="rect" href="http://svn.apache.org/repos/asf/cxf/trunk/security/CVE-2010-2076.pdf" data-linked-resource-id="2076" data-linked-resource-version="1" data-linked-resource-type="text/plain" data-linked-resource-container-id="2076" data-linked-resource-container-version="1">CVE-2010-2076</a> - DTD based XML attacks.</li></ul></div></div><!-- Content --></td>