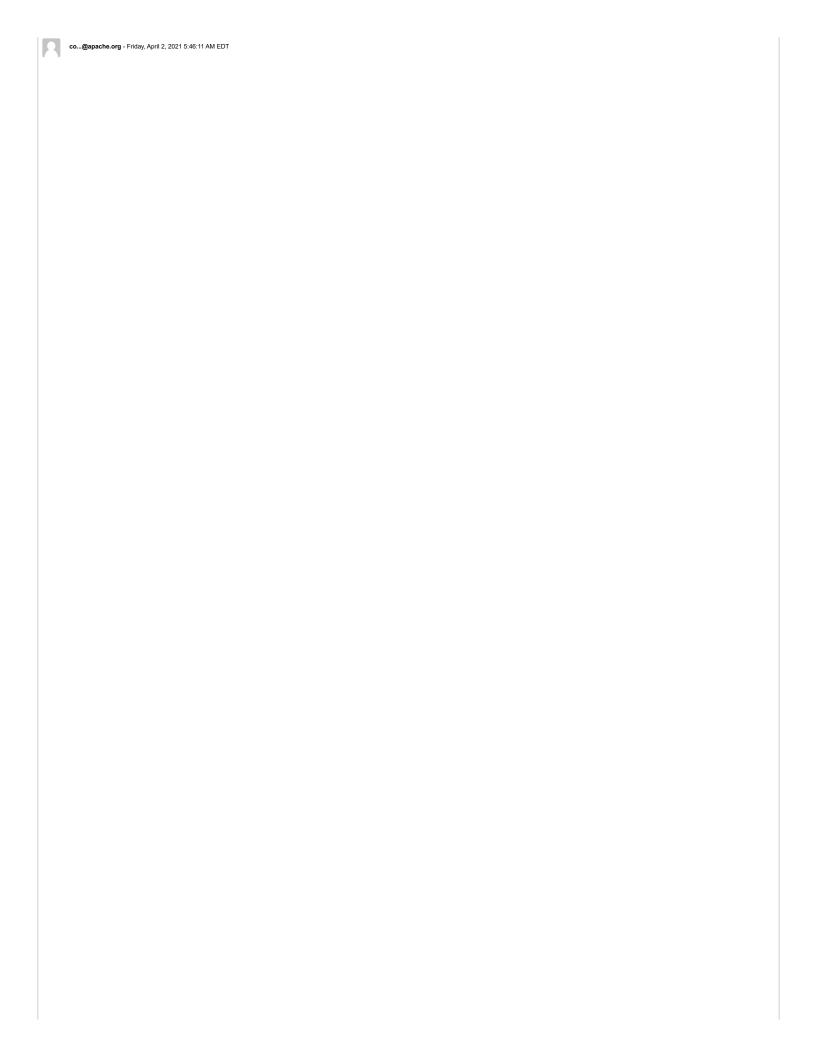
svn commit: r1073270 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2021-22696.txt.asc security-advisories.html	
Posted to commits@cxf.apache.org (list.html?commits@cxf.apache.org)	



Author: coheigea

Date: Fri Apr 2 09:46:11 2021

New Revision: 1073270

Log:
Adding security advisory

Added:
websites/production/cxf/content/security-advisories.data/CVE-2021-22696.txt.asc
Modified:
websites/production/cxf/content/cache/main.pageCache
websites/production/cxf/content/security-advisories.html

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

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

Binary files - no diff available.

\_\_\_\_\_\_

```
--- 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
+OAuth 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--
+iQEzBAEBCqAdFiEE20Xs0ZuXUU9ycQWuZ7+AsQrVOYMFAmBm444ACqkQZ7+AsQrV
+OYMP8Af+LKmoCnKzWikWNXphDIGrefAvKJNhpguBy6msBs8BRU+4kwGV5jjSaHpg
+1sYeDdxV1qQzWiRlXluyUIwLd+iY6FEYurC5ZAi9Mhd1M0B+iIfF1asxmVK+4Iyq
+NphtgDCFGAM0D60VFR5\DX0Ib6E1mM+gTKp\KMxY7NUJUw4mDRAAmQVrpkPzsNI/
+0E+zVFL8crotUOiDN0icUncaZt/i+P3iNFt5/77YrgMwgYcmuDTpSMzDtRPUiaaF
+svj/kI8x+U2e2BZRqUUYnJJMy2tmLKWw47d9/cGqJZ00qip/caFntDYsfECt13Z3
+bU+bEzRGdbEiTRS3mj1bSvwzK+RxZg==
+----END PGP SIGNATURE----
```

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

```
wodined. websites/production/cxi/content/security-advisories.ntml
```

```
--- 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
                                           <!-- Content -->
                                                     <div class="wiki-content">
 --<div id="ConfluenceContent">-\div id=3 \\div id=3 \\did=3 \\div id=3 \\div id=3 \\div id=3 \\div id=3 \\div id=3 \\div 
 advisories.data/CVE-2020-1954.txt.asc?version=1&modificationDate=1585730169000&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

attack

attack

 version=2& modificationDate=1584610519000& api=v2" data=linked-resource-default-alias="CVE-2019-17573.txt.asc" 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-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="38">CVE-2019-17573.txt.asc" data-nice-type="Text File" data-linked-resource-container-version="38">CVE-2019-17573.txt.asc" data-nice-type="Text File" data-linked-resource-container-version="38">CVE-2019-17573.txt.asc
 12423.txt.asc?version=1&modificationDate=1579178393000&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 privately-secret redentials if configured with a jwk keystore</ti>
keystore
keystore
li><a shape="rect" href="security-advisories. data/CVE-2019-12419.txt.asc?version=28amp;modificationDate=15729612018008amp;api=v2" data-linked-resource-data-linked-resource-default-alias="CVE-2019-12419.txt.asc" data-linked-resource-container-version="2" data-linked-resource-container-version="2" shape="rect" href="security-advisories.data/CVE-2019-12419.txt.asc" data-linked-resource-container-version="3" shape="rect" href="security-advisories.data/CVE-2019-12419.txt.asc" data-linked-resource-container-version="3" shape="rect" href="security-advisories.data/CVE-2019-12419.txt.asc" data-linked-resource-container-version="3" shape="rect" href="security-advisories.data-linked-resource-container-version="3" shape="rect" href="security-adv
 not properly validate the clientIda shape="rect" href="security-advisories.data/CVE-201" 9-12406.txt.asc?version=1& modificationDate=1572957147000& api=v2" data-linked-resource-id="135859607" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linke
 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
   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.
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-type="text/plain" data-linked-resource-default-alias="text/plain" data-linked-resource-id="text/plain" data-linked-res
 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.
 version=1&modificationDate=1510661632000&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-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-type="text/plain" da
   resource-container-version="38">CVE-2017-12624</a>: Apache CXF web services that process attachments are vulnerable to Denial of Service (DoS) attacks.
 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 Fedix 01DC Client Registration Service is vulnerable to CSFR attacks.
CSFR attacks
 Jetty and Spring plugins are vulnerable to CSRF attacks.<a shape="rect" href="security">jetty and Spring plugins are vulnerable to CSRF attacks.</a>
```

-advisories.data/CVE-2017-5656.txt.asc?version=1&modificationDate=1492515113000&api=v2" data-linked-resource-id="69406543" data-linked-resource-version="1" data-linkedresource-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>\sin shape="rect" href="security-advisories.data/CVE-2017-5653.txt.asc?version=16amp;modificationDate=14925150740006amp;api=v2" data-linked-resource-1de=04006542"
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-containerversion="38">CVE-2017-5653</a>: Apache CXF JAX-RS XML Security streaming clients do not validate that the service response was signed or encrypted.
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.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.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.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-version="38">CVE-2017-3156.txt.asc" data-nice-type="Text File" data-linked-resource-container-version="38">CVE-2017-3156.txt.asc timing attacks<h3 id="SecurityAdvisories-2016">2016</h3><a shape="rect" href="security-advisories.data/CVE-2016-8739.txt.asc? version=16amp;modificationDate=14821643600006amp;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 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-resourcecontainer-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<a shape="rect" href="security-advisories.data/CVE-2016-4464.txt.asc?version=1&amp;modificatio" href="security-advisories.data/cVE-2016-4464.txt.asc?version=1&amp;modification=1&amp;modi Date=14733501530006amp;api=v2" data-linked-resource-id="65860472" 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 id="SecurityAdvisories-2015">2015</hd>><a shape="rect" href="security-advisories.data/CVE-2015-5253.txt.asc?version=1&amp;modificationDate=14474333400006amp;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 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="38">CVE-2015-5175</a>: Apache CXF Fediz application plugins are vulnerable to Denial of Service (DoS) attacks<hr/>d="SecurityAdvisories-2014">2014</hr></hr> la="SecurityAdvisories-Z014">Z0144/ib>Z0144/ib>Z0144/ib>Z0144/ib>Z0144/ib>Z0144/ib>Z0144/ib>Z0144/ib>Z0144/ib>Z0144/ib>Z0144/ib>Z0144/ib>Z0144/ib>Z0142-ibide-resource-de"sila3657" data-liked-resource-de"sila3657" data-liked-resource-de fault-alias="CVE-2014-3577.txt.asc" data-nice-type="Text File" data-liked-resource-type="attachment" data-liked-resource-container-id="27837502" data-liked-resource-container-version="38"×CVE-2014-3576.43>: Apache CXF SSL hostname verification bypass
Vorsion=15&mg; modificationDate=14187404740806amp; api=v2" data-liked-resource-tod="59561078" data-liked-resource-version="15" data-liked-resource-tod="59561078" data-liked-resource-version="15" data-liked-resource-container-id="27837502" data-liked-resource-tod="59561078" data-liked-resource-tod="59561078" data-liked-resource-container-id="27837502" data-like resource-container-version="38">Note on CVE-2014-3566</a>: SSL 3.0 support in Apache CXF, aka the "POODLE" attack.
"attack.
"itack.
"attack.
"attack.< -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 TransportBinding4 sa 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 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 <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-</p> 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 00M errorserrorserrorsli><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-resou linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-0110.txt.asc" data-lice-type="Text File" data-linked-resourcecontent-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 version=16amp;modificationDate=13988733850006amp;api=v2" data-linked-resource-id="40895140" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-content-type="text/plain" data-linkedresource-container-version="38">CVE-2014-0034</a>: The SecurityTokenService accepts certain invalid SAML Tokens as valid
2014-0035.txt.asc?version=16amp;modificationDate=13988733910006Amp;api=v2" data-linked-resource-id="48095141" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-type="text/p" lain" data-linked-resource-container-type="text/p" lain" lain" data-linked-resource-container-type="text/p" lain" lain" data-linked-resource-container-type="text/p" lain" lain" data-linked-resource-container-type="text/p" lain" lain" lain" data-linked-resource-container-type="text/p" lain" la EncryptBeforeSigning policy
EncryptBeforeSigning policy
Figure 13723243010006amp; api=v2" data-linked-resource-id="33095710" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-resource-type="attachment 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-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-content-type="text/plain" data-linked-resource-content-type resource-container-version="38">CVE-2013-2160</a> - Denial of Service Attacks on Apache CXF
Apach as in the case of MS-SecurityPolicy enabled plaintext UsernameTokenes.
as in the case of MS-SecurityPolicy enabled plaintext UsernameTokenes.
as in the case of MS-SecurityPolicy enabled plaintext UsernameTokenes.
becautityAdvisories-2012">2012-5633
as in the case of MS-SecurityPolicy enabled plaintext UsernameTokenes.
c/li>
c/li>
c/s a shape="rect" href="rote-on-cve-2011-2487.html">Note on CVE-2011-2487.html">Note on CVE-2011-2487.html
d is comparable to SOAP Action spoofing attacks against distributed symmetric key in MS-Security.
c/li>
c/li>
c/s a shape="rect" href="rove-2012-2391.html">Note on CVE-2012-23451.html
c/li>
c/s is vulnerable to SOAP Action spoofing attacks on Document Literal web services.
c/li>
c/li>
c/s is vulnerable to SOAP Action spoofing attacks on Document Literal web services.
c/li>
c/s is vulnerable to SOAP Action spoofing attacks.
c/li>
c/s is vulnerable to SOAP Action spoofing attacks.
c/li>
c/s is vulnerable to SOAP Action spoofing attacks.
c/li>
c/s is vulnerable to SOAP Action spoofing attacks.
c/li>
c/s is vulnerable to SOAP Action spoofing attacks.
c/li>
c/s is vulnerable to SOAP Action spoofing attacks.
c/s is vulnerable to SOAP Action spoof ml">Note on CVE-2011-1096</a> - XML Encryption flaw / Character pattern encoding attack.a shape="rect" href="cve-2012-0803.html">CVE-2012-0803</a> - Apache CXF does not validate UsernameToken policies correctly./li><h3 id="SecurityAdvisories-2010">2010">2010</h3>a shape="rect" class="external-link" href="http://svn.apache.org/repos/asf/cxf/trunk/security/CVE-2010-2076.pdf">CVE-2010-2076.pdf</a> version=1&modificationDate=1617355743000&api=v2" data-linked-resource-id="177049091" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linkedresource-default-alias="CVE-2021-22696.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-2021-22696</a>: OAuth 2 authorization service vulnerable to DDos attacks shape="rect" href="security-advisories.data/CVE-2020-13954.txt.asc?version=1&modificationDate=1605183671000&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" dat a-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="39">CVE-2020-13954</a>: Apache CXF Reflected XSS in the services listing page via the styleSheetPath version=16amp;modificationDate=15857301690006amp;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-content-type="text/plain" data-linked-resource-co resource-container-version="39">CVE-2020-1954</a>: Apache CXF JMX Integration is vulnerable to a MITM attack<ha> id="SecurityAdvisories-2019">2019</ha></ha>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="39">CVE-2019-17573</a>: Apache CXF Reflected XSS in the services listing pagelista shape="rect" href="security-advisories.data/CVE-2019-12423.txt.asc?version=16amp;modificationDate=15791783939006amp;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-type="attachment" data-linked-resource-default-alias="CVE-2019-12423.txt.asc" data-nice-type="Text File" data-nice-t linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="39">CVE-2019-12423</a>: Apache CXF OpenId Connect JWK Keys service returns private/secret credentials if configured with a jwk keystore
keys service returns private/secret credentials if configured with a jwk keystore
ked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resource-id="135859612" data-linked-resource-version="2" data-linked-resource-id="135859612" data-linked-resourceresource-container-id="27837502" data-linked-resource-container-version="39">CVE-2019-12419</a>: Apache CXF OpenId Connect token service does not properly validate the clientId <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-contenttype="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="39"

-

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
XML attacks
XML of tacks
XML attacks
XML of tacks
XML attacks
XML attac

"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.
href="security-advisories data/CVE-2017-7662.txt.asc?version=18.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.txt.asc" data-linked-resource-content-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="1" data-linked-resource-type="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="1" data-linked-resource-type="text/plain" data-linked-resource-container-version="1" data-linked-resource-type="text/plain" data-linked-resource-type="text/plain" data-linked-resource-type="text/plain" data-linked-resource-type="text/plain" data-linked-resource-type="text/plain" data-linked-resource-type="text/plain" data-linked-

< 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-container-id="27837502" data-lin

VERSION = 37 PCVC-2017-70015/aP. THE APACHE CAF FEUIZ JETUS BRU SPHING PROGRES ARE VUINERABLE TO COME ATTACKS. SHIPS A SHAPE FECT. THEFE SECURITY-AUVISORES. GRADULT AND ACCUSED AND ACCUS

version=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-2017-5656.txt.asc" data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linke

ontainer-version="39">CVE-2017-5656</a>: Apache CXF's STSClient uses a flawed way of caching tokens that are associated with delegation tokens.
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.btt.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.
vi><a shape="rect" href="security-advisories.data/CVE-2017-3156.btt.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-type="attachment" data-linked-resource-type="attachment" data-linked-resource-type="attachment" data-linked-resource-type="attachment" data-linked-resource-type="attachment" data-linked-resource-type="attachment" data-linked-resource-type="attachment" data-linked-resource-container-id="27837502" data-linked-resource-container-version="39">
attachment data-linked-resource-type="attachment" data-linked-resource-container-id="27837502" data-linked-resource-container-version="39">
attachment data-linked-resource-type="attachment" data-linked-resource-container-id="27837502" data-linked-resource-container-version="39">
attachment data-linked-resource-type="attachment" data-linked-resource-container-id="27837502" data-linked-resource-container-version="39">
attachment data-linked-resource-container-id="27837502" data-linked-resource-container-id="27837502" data-linked-resource-container-id="27837502" data-linked-resource-container-id="27837502" data-linked-resource-container-id="27837502" data-linked-resource-container-id="27837502" data-linked-resource-container-id="27837502" data-linked-resour

source-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> 
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li> 
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks-/li>
Apache CXF OAuth2 Hawk and JOSE MAC Vali

&amp,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-version="39">CVE-2016-6812</a>: XSS risk in Apache CXF FormattedServiceListWriter when a request URL contains matrix parameters
(ii> < ii> < 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-container-version="1" data-linked-resource-container-version="1" data-linked-resource-container-version="1" data-linked-resource-container-version="1" data-linked-resource-container-version="39">CVE-2016-4464.txt.asc" data-nice-type="Text File" data-linked-resource-container-version="39">CVE-2016-4464.txt.asc" data-nice-type="

ation plugins do not match the SAML AudienceRestriction values against the list of configured audience URIs</i>
5253.txt.asc?version=1&amp;modificationDate=1447433340000&amp;api=2" data-linked-resource-id="f1326642" data-linked-resource-version="1" data-linked-resource-type="atachment" 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
\$\f(li) < a \text{sape} = \text{"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="39">CVE-2015-5175</a>: Apache CXF Fediz application plugins are vulnerable to Denial of Service (DoS) attacks

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-version="39">CVE-2014-3577 </a>: Apache CXF SSL hostname verification bypass

nked-resource-id="50561078" data-linked-resource-version="1" 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. 
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. 
data-linked-resource-version="1" data-linked-resource-ve

data-nice-type="Text File" data-linked-resource-content-type="text/plain" data-linked-resource-container-vid="27 837502" data-linked-resource-container-version="39">CVE-2014-0109</a>. HTML content posted to SOAP endpoint could cause OOM errors
837502" data-linked-resource-container-version="39">CVE-2014-0109</a>. HTML content posted to SOAP endpoint could cause OOM errors
837502" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-0110.txt.asc" data-linked-resource-type="attachment" data-linked-resource-default-alias="CVE-2014-0110.txt.asc" data-nice-type="Text File" data-linked-resource-container-version="39">CVE-2014-0110</a>. Large invalid content could cause temporary space to fill
836702" data-linked-resource-container-version="39">CVE-2014-0110</a>. Large invalid content could cause temporary space to fill
8367038873385000&amp;api=v2" data-linked-resource-id="40895140" data-linked-resource-version="1" data-linked-resource-default-alias="CVE-2014-0034.txt.asc?version=18.amp;modificationDate=1398873385000&amp;api=v2" data-linked-resource-id="40895140" data-linked-resource-version="1" data-linked-resource-default-alias="CVE-2014-0034.txt.asc?version=18.amp;modificationDate=1398873385000&amp;api=v2" data-linked-resource-id="40895140" data-linked-resource-version="1" data-linked-resource-default-alias="CVE-2014-0034.txt.asc?version=18.amp;modificationDate=1398873385000&amp;api=v2" data-linked-resource-id="40895140" data-linked-resource-version="1" data-linked-resource-id="40895140" data-linked-resource-id="40895140" data-linked-resource-version="1" data-linked-resource-id="40895140" data-linked-resource-id="40895140" data-linked-resource-version="1" data-linked-resource-id="40895140" data-linked-resource-id="40895140" data-linked-resource-id="40895140" data-linked-resource-id="40895140" data-linked-resource-id="40895140" data-linked-resource-id="40895140" data-linked-resource-id="40895140" data-linked-resource-id="40895140" data-linked-resourc

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 
<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="text/plain" data-linked-resource-container-id="27837502" data-linked-resource-container-version="3">CVE-2014-0035.txt.asc?version=1%amp;modificationDate=1398873391000&amp;api=v2" data-linked-resource-id="40895141" data-linked-resource-container-id="27837502" data-linked-resource-conta

d="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-d="27837502" data-linked-resource-container-version="39">CVE-2013-2160./a> - Denial of Service Attacks on Apache CXF
Encryption backwards compatibility attack on Apache CXF.
As shape="rect" href="cve-2013-0239.html">CVE-2013-0239.html">CVE-2013-0239.html">CVE-2013-0239.html
CVE-2013-0239.html
CVE-2013-02

S-Security. 
S-Security.

</div>
<!-- Content -->