svn commit: r1075801 - in /websites/production/cxf/content: cache/main.pageCache index.html security-advisories.data/CVE-2021-30468.txt.asc security-advisories.html

co...@apache.org - Wednesday, June 16, 2021 5:27:41 AM EDT

Author: coheigea
Date: Wed Jun 16 09:27:41 2021
New Revision: 1075801

Log:
Adding security advisory

Added:
websites/production/cxf/content/security-advisories.data/CVE-2021-30468.txt.asc
Modified:
websites/production/cxf/content/cache/main.pageCache
websites/production/cxf/content/index.html
websites/production/cxf/content/security-advisories.html

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

Modified: websites/production/cxf/content/index.html
==

```
--- websites/production/cxf/content/index.html (original)
+++ websites/production/cxf/content/index.html Wed Jun 16 09:27:41 2021
@@ -99,7 +99,7 @@ Apache CXF -- Index
          <td height="100%">
            <!-- Content -->
            <div class="wiki-content">
-<div id="ConfluenceContent"><h1 id="Index-ApacheCXF&#8482;:AnOpen-SourceServicesFramework">Apache CXF&#8482;: An Open-Source Services Framework</h1><h2 id="Index-
Overview">Overview</h2><p>Apache CXF&#8482; is an open source services framework. CXF helps you build and develop services using frontend programming APIs, like JAX-WS and JAX-RS.
These services can speak a variety of protocols such as SOAP, XML/HTTP, RESTful HTTP, or CORBA and work over a variety of transports such as HTTP, JMS or JBI.</p><h2 id="Index-
News">News</h2><h3 id="Index-June8,2021-ApacheCXF3.4.4and3.3.11released!">June 8, 2021 - Apache CXF 3.4.4 and 3.3.11 released!</h3><p>The Apache CXF team is proud to announce the
availability of our latest patch releases!  Over 26 JIRA issues were fixed for 3.4.4, many back ported to 3.3.11.</p><p>Downloads are available <a shape="rect"
href="download.html">here</a>.</p><h3 id="Index-March22,2021-ApacheCXF3.4.3and3.3.10released!">March 22, 2021 - Apache CXF 3.4.3 a
 nd 3.3.10 released!</h3><p>The Apache CXF team is proud to announce the availability of our latest patch releases!  Over 22 JIRA issues were fixed for 3.4.3, many back ported
to 3.3.10.</p><p>Downloads are available <a shape="rect" href="download.html">here</a>.</p><h3 id="Index-Features">Features</h3><p>CXF includes a broad feature set, but it is
primarily focused on the following areas:</p><ul><li><strong>Web Services Standards Support:</strong> CXF supports a variety of web service standards including SOAP, the WS-I Basic
Profile, WSDL, WS-Addressing, WS-Policy, WS-ReliableMessaging, WS-Security, WS-SecurityPolicy, WS-SecureConverstation, and WS-Trust (partial).</li><li><strong>Frontends:</strong>
CXF supports a variety of "frontend" programming models.</li></ul><p>CXF implements the JAX-WS APIs. CXF JAX-WS support includes some extensions to the standard that make it
significantly easier to use, compared to the reference implementation: It will automatically generate c
 ode for request and response bean classes, and does not require a WSDL for simple cases.</p><p>It also includes a "simple frontend" which allows creation of clients and endpoints
without annotations. CXF supports both contract first development with WSDL and code first development starting from Java.</p><p>For REST, CXF also supports a JAX-RS frontend.</p>
<ul><li><strong>Ease of use:</strong> CXF is designed to be intuitive and easy to use. There are simple APIs to quickly build code-first services, Maven plug-ins to make tooling
integration easy, JAX-WS API support, Spring 2.x XML support to make configuration a snap, and much more.</li><li><strong>Binary and Legacy Protocol Support:</strong> CXF has been
designed to provide a pluggable architecture that supports not only XML but also non-XML type bindings, such as JSON and CORBA, in combination with any type of transport.</li></ul>
<p>To get started using CXF, check out the <a shape="rect" href="download.html">downloads</a>, the <a
  shape="rect" href="http://cxf.apache.org/docs/index.html">user's guide</a>, or the <a shape="rect" href="mailing-lists.html">mailing lists</a> to get more information!</p><h2
id="Index-Goals">Goals</h2><h3 id="Index-General">General</h3><ul><li>High Performance</li><li>Extensible</li><li>Intuitive &amp; Easy to Use</li></ul><h3 id="Index-
SupportforStandards">Support for Standards</h3><h5 id="Index-JSRSupport">JSR Support</h5><ul><li>JAX-WS - Java API for XML-Based Web Services (JAX-WS) 2.0 - <a shape="rect"
class="external-link" href="http://jcp.org/en/jsr/detail?id=224" rel="nofollow">JSR-224</a></li><li>Web Services Metadata for the Java Platform - <a shape="rect" class="external-
link" href="http://jcp.org/en/jsr/detail?id=181" rel="nofollow">JSR-181</a></li><li>JAX-RS - The Java API for RESTful Web Services - <a shape="rect" class="external-link"
href="http://jcp.org/en/jsr/detail?id=311" rel="nofollow">JSR-311,</a> <a shape="rect" class="external-link" href="https://jcp.org/en/
 jsr/detail?id=370" rel="nofollow">JSR-370</a></li><li>SAAJ - SOAP with Attachments API for Java (SAAJ) - <a shape="rect" class="external-link"
href="http://jcp.org/aboutJava/communityprocess/mrel/jsr067/index3.html" rel="nofollow">JSR-67</a></li></ul><h5 id="Index-WS-*andrelatedSpecificationsSupport">WS-* and related
Specifications Support</h5><ul><li>Basic support: WS-I Basic Profile 1.1</li><li>Quality of Service: WS-Reliable Messaging</li><li>Metadata: WS-Policy, WSDL 1.1 - Web Service
Definition Language</li><li>Communication Security: WS-Security, WS-SecurityPolicy, WS-SecureConversation, WS-Trust (partial support)</li><li>Messaging Support: WS-Addressing, SOAP
1.1, SOAP 1.2, Message Transmission Optimization Mechanism (MTOM)</li></ul><h5 id="Index-OpenAPISpecification(OAS)Support">OpenAPI Specification (OAS) Support</h5><ul><li>OAS 2.0
(classic Swagger specification)</li><li>OAS 3.0.x (new revised specification)</li></ul><h3 id="Index-MultipleTransports,ProtocolBindings,DataBi
 ndings,andFormats">Multiple Transports, Protocol Bindings, Data Bindings, and Formats</h3><ul><li>Transports: HTTP, Servlet, JMS, In-VM and many others via the <a shape="rect"
class="external-link" href="http://camel.apache.org/camel-transport-for-cxf.html">Camel transport for CXF</a> such as SMTP/POP3, TCP and Jabber</li><li>Protocol Bindings: SOAP,
REST/HTTP, pure XML</li><li>Data bindings: JAXB 2.x, Aegis, Apache XMLBeans, Service Data Objects (SDO), JiBX</li><li>Formats: XML Textual, JSON, FastInfoset</li><li>Extensibility
API allows additional bindings for CXF, enabling additional message format support such as CORBA/IIOP</li></ul><h3 id="Index-FlexibleDeployment">Flexible Deployment</h3><ul>
<li>Lightweight containers: deploy services in Jetty, Tomcat or Spring-based containers</li><li>JBI integration: deploy as a service engine in a JBI container such as ServiceMix,
OpenESB or Petals</li><li>Java EE integration: deploy services in Java EE application servers such as Apache Ger
 onimo, JOnAS, Redhat JBoss, OC4J, Oracle WebLogic, and IBM WebSphere</li><li>Standalone Java client/server</li></ul><h3 id="Index-SupportforMultipleProgrammingLanguages">Support
for Multiple Programming Languages</h3><ul><li>Full support for JAX-WS 2.x client/server programming model</li><li>JAX-WS 2.x synchronous, asynchronous and one-way API's</li>
<li>JAX-WS 2.x Dynamic Invocation Interface (DII) API</li><li>JAX-RS for RESTful clients</li><li>Support for wrapped and non-wrapped styles</li><li>XML messaging API</li><li>Support
for JavaScript and ECMAScript 4 XML (E4X) - both client and server</li><li>Support for CORBA</li><li>Support for JBI with ServiceMix</li></ul><h3 id="Index-Tooling">Tooling</h3><ul>
<li>Generating Code: WSDL to Java, WSDL to JavaScript, Java to JavaScript</li><li>Generating WSDL: Java to WSDL, XSD to WSDL, IDL to WSDL, WSDL to XML</li><li>Adding Endpoints: WSDL
to SOAP, WSDL to CORBA, WSDL to service</li><li>Generating Support Files: WSDL to IDL</li><li>Valida
 ting Files: WSDL Validation</li></ul><h2 id="Index-GettingInvolved">Getting Involved</h2><p>Apache CXF is currently under heavy development. To get involved you can <a shape="rect"
href="mailing-lists.html">subscribe to the mailing lists</a>. You can also grab the code from the <a shape="rect" href="source-repository.html">Source Repository</a>. You also need
to read about <a shape="rect" href="building.html">Building</a> CXF. For Eclipse users, you should read about <a shape="rect" href="setting-up-eclipse.html">Setting up Eclipse</a>.
</p></div>
+<div id="ConfluenceContent"><h1 id="Index-ApacheCXF&#8482;:AnOpen-SourceServicesFramework">Apache CXF&#8482;: An Open-Source Services Framework</h1><h2 id="Index-
Overview">Overview</h2><p>Apache CXF&#8482; is an open source services framework. CXF helps you build and develop services using frontend programming APIs, like JAX-WS and JAX-RS.
These services can speak a variety of protocols such as SOAP, XML/HTTP, RESTful HTTP, or CORBA and work over a variety of transports such as HTTP, JMS or JBI.</p><h2 id="Index-
News">News</h2><h3 id="Index-June8,2021-ApacheCXF3.4.4and3.3.11released!">June 8, 2021 - Apache CXF 3.4.4 and 3.3.11 released!</h3><p>The Apache CXF team is proud to announce the
availability of our latest patch releases!  Over 26 JIRA issues were fixed for 3.4.4, many back ported to 3.3.11.</p><p>These releases contain a fix for a security issue,
please see the <a shape="rect" href="security-advisories.html">security advisories</a> page for more information:</p><ul><li
```

ong>Frontends: CXF supports a variety of "frontend" programming models. CXF implements the JAX-WS APIs. CXF JAX-WS support includes some extensions to the standard that make it significantly easier to use, compared to the reference implementation: It will automatically generate code for request and response bean classes, and does not require a WSDL for simple cases. It also includes a "simple frontend" which allows creation of clients and endpoints without annotations. CXF supports both contract first development with WSDL and code first development starting from Java. For REST, CXF also supports a JAX-RS frontend. Ease of use: CXF is designed to be intuitive and easy to use. There are simple APIs to quickly build code-first services, Maven plug-ins to make tooling integration easy, JAX-WS API support, Spring 2.x XML support to make configuration a snap, and much more.
Binary and Legacy Protocol Support:</s
trong> CXF has been designed to provide a pluggable architecture that supports not only XML but also non-XML type bindings, such as JSON and CORBA, in combination with any type of transport. To get started using CXF, check out the downloads, the user's guide, or the mailing lists to get more information! <h2 id="Index-Goals">Goals</h2><h3 id="Index-General">General</h3>
High Performance
Extensible
Intuitive & Easy to Use
<h3 id="Index-SupportforStandards">Support for Standards</h3><h5 id="Index-JSRSupport">JSR Support</h5>
JAX-WS - Java API for XML-Based Web Services (JAX-WS) 2.0 - JSR-224
Web Services Metadata for the Java Platform - <a shape="rect" class="external-link
" href="http://jcp.org/en/jsr/detail?id=181 (http://jcp.org/en/jsr/detail?id=181)" rel="nofollow">JSR-181
JAX-RS - The Java API for RESTful Web Services - JSR-311, JSR-370
SAAJ - SOAP with Attachments API for Java (SAAJ) - JSR-67
<h5 id="Index-WS-*andrelatedSpecificationsSupport">WS-* and related Specifications Support</h5>
Basic support: WS-I Basic Profile 1.1
Quality of Service: WS-Reliable Messaging
Metadata: WS-Policy, WSDL 1.1 - Web Service Definition Language
Communication Security: WS-Security, WS-SecurityPolicy, WS-SecureConversation, WS-Trust (partial support)
Messaging Support: WS-Addressing, SOAP 1.1, SOAP 1.2, Messag
e Transmission Optimization Mechanism (MTOM)
<h5 id="Index-OpenAPISpecification(OAS)Support">OpenAPI Specification (OAS) Support</h5>
OAS 2.0 (classic Swagger specification)
OAS 3.0.x (new revised specification)
<h3 id="Index-MultipleTransports,ProtocolBindings,DataBindings,andFormats">Multiple Transports, Protocol Bindings, Data Bindings, and Formats</h3>
Transports: HTTP, Servlet, JMS, In-VM and many others via the Camel transport for CXF such as SMTP/POP3, TCP and Jabber
Protocol Bindings: SOAP, REST/HTTP, pure XML
Data bindings: JAXB 2.x, Aegis, Apache XMLBeans, Service Data Objects (SDO), JiBX
Formats: XML Textual, JSON, FastInfoset
Extensibility API allows additional bindings for CXF, enabling additional message format support such as CORBA/IIOP
<h3 id="Index-FlexibleDeploymen
t</h3>
Lightweight containers: deploy services in Jetty, Tomcat or Spring-based containers
JBI integration: deploy as a service engine in a JBI container such as ServiceMix, OpenESB or Petals
Java EE integration: deploy services in Java EE application servers such as Apache Geronimo, JOnAS, Redhat JBoss, OC4J, Oracle WebLogic, and IBM WebSphere
Standalone Java client/server
<h3 id="Index-SupportforMultipleProgrammingLanguages">Support for Multiple Programming Languages</h3>
Full support for JAX-WS 2.x client/server programming model
JAX-WS 2.x synchronous, asynchronous and one-way

API's
JAX-WS 2.x Dynamic Invocation Interface (DII) API
JAX-RS for RESTful clients
Support for wrapped and non-wrapped styles
XML messaging API
Support for JavaScript and ECMAScript 4 XML (E4X) - both client and server
Support for CORBA
Support for JBI with ServiceMix
<h3 id="Index-Toolin
g">Tooling</h3>
Generating Code: WSDL to Java, WSDL to JavaScript, Java to JavaScript
Generating WSDL: Java to WSDL, XSD to WSDL, IDL to WSDL, WSDL to XML
Adding Endpoints: WSDL to SOAP, WSDL to CORBA, WSDL to service
Generating Support Files: WSDL to IDL
Validating Files: WSDL Validation
<h2 id="Index-GettingInvolved">Getting Involved</h2> Apache CXF is currently under heavy development. To get involved you can subscribe to the mailing lists. You can also grab the code from the Source Repository. You also need to read about Building CXF. For Eclipse users, you should read about Setting up Eclipse.

<!-- Content -->
</td>

Added: websites/production/cxf/content/security-advisories.data/CVE-2021-30468.txt.asc
==========

```
--- websites/production/cxf/content/security-advisories.data/CVE-2021-30468.txt.asc (added)
+++ websites/production/cxf/content/security-advisories.data/CVE-2021-30468.txt.asc Wed Jun 16 09:27:41 2021
@@ -0,0 +1,30 @@
+-----BEGIN PGP SIGNED MESSAGE-----
+Hash: SHA512
+
+Apache CXF Denial of service vulnerability in parsing JSON via JsonMapObjectReaderWriter (CVE-2021-30468)
+
+PRODUCT AFFECTED:
+
+This issue affects Apache CXF.
+
+PROBLEM:
+
+A vulnerability in the JsonMapObjectReaderWriter of Apache CXF allows an
+attacker to submit malformed JSON to a web service, which results in the thread
+getting stuck in an infinite loop, consuming CPU indefinitely.
+
+This issue affects Apache CXF versions prior to 3.4.4; Apache CXF versions
+prior to 3.3.11.
+
+This issue has been assigned CVE-2021-30468.
+-----BEGIN PGP SIGNATURE-----
+
+iQEzBAEBCgAdFiEE20Xs0ZuXUU9ycQWuZ7+AsQrVOYMFAmDJwpQACgkQZ7+AsQrV
+OYMsSwgAsYUMH9tHgKEKK9TG74ejNZQ/nKDw6P5lw9X3IgEi7oDXPoZuvJjaTWVn
+EKcACu7jFoolhjPtuXjO7ZFXzm0huzqXJwJSx6H+y1HAcDKZAkCnKn9S2omF0wzf
+IQJnw4foABDCQyV63BiYiGTKpN6kWNqb2E3TLE8ZfjTllhvDXZIojLbdxLhWdMCh
+neKW1MgLDoeObjIde3K28NyH+6Y2MBJAnEJ/duZ7T/igRqUn+i/MyV1q2eVe3JbX
+mo+sKDrnxmo09IuzcRafEd/mIJOw4KokcaWNFUswOMtRCLetw7Q0XIGyNjcIHsjW
+LaETfe3x7ctxTPQwAlMqF2jREXJRHA==
+=wnm/
+-----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 Wed Jun 16 09:27:41 2021
@@ -99,7 +99,7 @@ Apache CXF -- Security Advisories
          <td height="100%">
            <!-- Content -->
            <div class="wiki-content">
-<div id="ConfluenceContent"><h3 id="SecurityAdvisories-2021">2021</h3><ul><li><a shape="rect" href="security-advisories.data/CVE-2021-22696.txt.asc?
version=1&amp;modificationDate=1617355743000&amp;api=v2" data-linked-resource-id="177049091" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-
resource-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</li></ul><h3 id="SecurityAdvisories-2020">2020</h3><ul><li><a
shape="rect" href="security-advisories.data/CVE-2020-13954.txt.asc?version=1&amp;modificationDate=1605183671000&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" 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</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="text/plain" data-linked-resource-container-id="27837502" data-linked-
resource-container-version="39">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="39">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="39">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="secu
 rity-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="39">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="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</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><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-c
ontainer-version="39">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="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&amp;modificationDate=1487590374000&amp;api=v2" data-linked-
resource-id="68715428" data-linked-resource-version="1" data-linked-resource-type="attachment" data-linked-re
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></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="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
```

resource-container-id="27837502" data-linked-resource-container-version="40">CVE-2016-4464: Apache CXF Fediz application plugins do not match the SAML AudienceRestriction values against the list of configured audience URIs
<h3 id="SecurityAdvisories-2015">2015</h3>
CVE-2015-5253: Apache CXF SAML SSO processing is vulnerable to a wrapping attack
CVE-2015-5175: Apache CXF Fediz application plugins are vulnerable to Denial of Service (DoS) attacks
<h3 id="SecurityAdvisories-2014">2014</h3>
CVE-2014-3577: Apache CXF SSL hostname verification bypass
Note on CVE-2014-3566: SSL 3.0 support in Apache CXF, aka the "POODLE" attack.
CVE-2014-3623: Apache CXF does not properly enforce the security semantics of SAML SubjectConfirmation methods when used with the TransportBinding
CVE-2014-3584: Apache CXF JAX-RS SAML handling is vulnerable to a Denial of Service (DoS) attack
CVE-2014-0109: HTML content posted to SOAP endpoint could cause OOM errors
CVE-2014-0110: Large invalid content could cause temporary space to fill
CVE-2014-0034: The SecurityTokenService accepts certain invalid SAML Tokens as valid
CVE-2014-0035: UsernameTokens are sent in plaintext with a Symmetric EncryptBeforeSigning policy
<h3 id="SecurityAdvisories-2013">2013</h3>
CVE-2013-2160 - Denial of Service Attacks on Apache CXF
Note on CVE-2012-5575 - XML Encryption backwards compatibility attack on Apache CXF.
CVE-2013-0239 - Authentication bypass in the case of WS-SecurityPolicy enabled plaintext UsernameTokens.
<h3 id="SecurityAdvisories-2012">2012</h3>
CVE-2012-5633 - WSS4JInInterceptor always allows HTTP Get requests from browser.
Note on CVE-2011-2487 - Bleichenbacher attack against distributed symmetric key in WS-Security.
CVE-2012-3451 - Apache CXF is vulnerable to SOAP Action spoofing attacks on Document Literal web services.
CVE-2012-2379 - Apache CXF does not verify that elements were signed or encrypted by a particular Supporting Token.
CVE-2012-2378 - Apache CXF does not pick up some child policies of WS-SecurityPolicy 1.1 SupportingToken policy assertions on the client side.
Note on CVE-2011-1096 - XML Encryption flaw / Character pattern encoding attack.
CVE-2012-0803 - Apache CXF does not validate UsernameToken policies correctly.
<h3 id="SecurityAdvisories-2010">2010</h3>
CVE-2010-2076 - DTD based XML attacks.

<!-- Content -->
</td>