Security Advisories

2018

- CVE-2018-8039: Apache CXF TLS hostname verification does not work correctly with com.sun.net.ssl.
- CVE-2018-8038: Apache CXF Fediz is vulnerable to DTD based XML attacks

2017

- CVE-2017-12631: CSRF vulnerabilities in the Apache CXF Fediz Spring plugins.
- CVE-2017-12624: Apache CXF web services that process attachments are vulnerable to Denial of Service (DoS) attacks.
- CVE-2017-7662: The Apache CXF Fediz OIDC Client Registration Service is vulnerable to CSRF attacks.
- CVE-2017-7661: The Apache CXF Fediz Jetty and Spring plugins are vulnerable to CSRF attacks.
- CVE-2017-5656: Apache CXF's STSClient uses a flawed way of caching tokens that are associated with delegation tokens.
- CVE-2017-5653: Apache CXF JAX-RS XML Security streaming clients do not validate that the service response was signed or encrypted.
- CVE-2017-3156: Apache CXF OAuth2 Hawk and JOSE MAC Validation code is vulnerable to the timing attacks

2016

- CVE-2016-8739: Atom entity provider of Apache CXF JAX-RS is vulnerable to XXE
- CVE-2016-6812: XSS risk in Apache CXF FormattedServiceListWriter when a request URL contains matrix parameters
- CVE-2016-4464: Apache CXF Fediz application plugins do not match the SAML AudienceRestriction values against the list of configured audience URIs

2015

- 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

2014

- 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

2013

- 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.

2012

- 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.

2010

- CVE-2010-2076 - DTD based XML attacks.