Security Advisories

2019

- CVE-2019-0188 - Apache Camel-XMLJson vulnerable to XML external entity injection (XXE)
- CVE-2019-0194 - Apache Camel's File is vulnerable to directory traversal

2018

- CVE-2018-8041 - Apache Camel's Mail is vulnerable to path traversal
- CVE-2018-8027 - Apache Camel's Core is vulnerable to XXE in XSD validation processor

2017

- CVE-2017-12634 - Apache Camel's Castor unmarshalling operation is vulnerable to Remote Code Execution attacks
- CVE-2017-12633 - Apache Camel's Hessian unmarshalling operation is vulnerable to Remote Code Execution attacks
- CVE-2017-5643 - Apache Camel's Validation Component is vulnerable against SSRF via remote DTDs and XXE
- CVE-2017-3159 - Apache Camel's Snakeyaml unmarshalling operation is vulnerable to Remote Code Execution attacks

2016

- CVE-2016-8749 - Apache Camel's Jackson and JacksonXML unmarshalling operation are vulnerable to Remote Code Execution attacks

2015

- CVE-2015-5344 - Apache Camel's XStream usage is vulnerable to Remote Code Execution attacks.
- CVE-2015-5348 - Apache Camel's Jetty/Servlet usage is vulnerable to Java object de-serialisation vulnerability.
- CVE-2015-0264 - The XPath handling in Apache Camel for invalid XML Strings or invalid XML GenericFile objects allows remote attackers to read arbitrary files via an XML External Entity (XXE) declaration. The XML External Entity (XXE) will be resolved before the Exception is thrown.
- CVE-2015-0263 - The XML converter setup in Apache Camel allows remote attackers to read arbitrary files via an SAXSource containing an XML External Entity (XXE) declaration.

2014

- CVE-2014-0003 - The Apache Camel XSLT component allows XSL stylesheets to perform calls to external Java methods.
- CVE-2014-0002 - The Apache Camel XSLT component will resolve entities in XML messages when transforming them using an xslt route.

2013

- CVE-2013-4330 - Writing files using FILE or FTP components, can potentially be exploited by a malicious user.