secadv

For information on how to report a new security problem please see here. The following security advisories have been issued in connection with the Santuario Project.

2023

- CVE-2023-44483: Apache Santuario: Private Key disclosure in debug-log output

2021

- CVE-2021-40690: Bypass of the secureValidation property

2019

- CVE-2019-12400: Apache Santuario potentially loads XML parsing code from an untrusted source

2014

- CVE-2014-8152: Streaming XML Signature verification failure

2013

- CVE-2013-4517: Java XML Signature DoS Attack
- CVE-2013-2210: Apache Santuario XML Security for C++ contains a heap overflow during XPointer evaluation
- CVE-2013-2172: Java XML Signature spoofing attack
- CVE-2013-2153: Apache Santuario XML Security for C++ contains an XML Signature Bypass issue
- CVE-2013-2154: Apache Santuario XML Security for C++ contains a stack overflow during XPointer evaluation
- CVE-2013-2155: Apache Santuario XML Security for C++ contains denial of service and hash length bypass issues while processing HMAC signatures
- CVE-2013-2156: Apache Santuario XML Security for C++ contains heap overflow while processing InclusiveNamespace PrefixList

2011

- CVE-2011-2516: Apache Santuario XML Security for C++ contains buffer overflows signing or verifying with large keys.