

old_news

Old News

November 2023

Version 4.0.1 of the Apache XML Security for Java library has been released, containing a bug fix (SANTUARIO-609 - Remove call to `Signature.getProvider()` in debug log)

October 2023

Versions 4.0.0, 3.0.3, 2.3.4 and 2.2.6 of the Apache XML Security for Java library have been released. A security advisory has been fixed in these releases:

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

Please see the [Security Advisories](#) page for more information.

September 2023

Version 4.0.0-M1 of the Apache XML Security for Java library has been released. This is a preview release of the forthcoming 4.0.0 release which is made available for testing, it should not be used in production. The main changes are:

- Java 11 requirement
- Removing SLF4J and using System.Logger
- AutoCloseable for several types

August 2023

Version 2.2.5 of the Apache XML Security for Java library has been released. It contains some dependency updates to fix CVE reports.

March 2023

Versions 3.0.2 and 2.3.3 of the Apache XML Security for Java library have been released. Support for the EdDSA has been added as part of these releases.

September 2022

Versions 3.0.1 and 2.3.2 of the Apache XML Security for Java library have been released. The main change is to remove Xalan as a provided (optional) dependency. This means that support for the XML Signature `here()` function is removed by default, but can be configured if needed (see [this test](#) for an example which plugs in this [custom XPath implementation](#)).

May 2022

Versions 3.0.0, 2.3.1, 2.2.4 and 2.1.8 of the Apache XML Security for Java library have been released. 3.0.0 is a new major release of the library that contains a change to the jakarta JAXB namespace for the streaming library. 2.1.8 is the last planned release of 2.1.x.

November 2021

Version 2.3.0 of the Apache XML Security for Java library has been released. This is a major new release of the library. Some of the significant changes include:

- A rewrite for the StAX output processor chain to make it deterministic - <https://issues.apache.org/jira/browse/SANTUARIO-555>
- Secure Validation is now enabled by default - <https://issues.apache.org/jira/browse/SANTUARIO-574>
- Local + HTTP ResourceResolvers are disabled by default - <https://issues.apache.org/jira/browse/SANTUARIO-573>

October 2021

Version 2.0.3 of the Apache XML Security for C++ library has been released. This release adds support for OpenSSL 3.0.0, though using a number of now-deprecated function calls.

September 2021

Version 2.2.3 and 2.1.7 of the Apache XML Security for Java library has been released. Please see the [release notes](#) for more information.

These releases contain a fix for a new CVE:

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

Please refer to the [security advisories](#) page for further information.

May 2021

Version 2.2.2 of the Apache XML Security for Java library has been released to fix a few bugs.

Please see the [release notes](#) for more information.

November 2020

Version 2.2.1 and 2.1.6 of the Apache XML Security for Java library have been released to fix a few bugs.

Please see the [release notes](#) for more information.

June 2020

Version 2.2.0 of the Apache XML Security for Java library has been released. This is a new major release with the following features:

- Added support for RSASSA-PSS with Parameters
- Extensive refactoring and code simplification
- JDK14 officially supported
- Ability to set a security provider when using org.apache.xml.security.signature.XMLSignature
- Added support for customizing how to parse a InputStream into a DOM Document

This release includes a fix for [CVE-2020-2773](#) which also affects our code base. However we will not be issuing a separate CVE, as we do not consider it a security vulnerability.

Please see the [release notes](#) for more information.

March 2020

Version 2.1.5 of the Apache XML Security for Java library has been released.

Please see the [release notes](#) for more information.

August 2019

Version 2.1.4 of the Apache XML Security for Java library has been released.

This release contains a fix for a security advisory - CVE-2019-12400: Apache Santuario potentially loads XML parsing code from an untrusted source. Please see the [security advisories](#) page for more information.

Please see the [release notes](#) for more information.

March 2019

Version 2.1.3 of the Apache XML Security for Java library has been released.

Please see the [release notes](#) for more information.

November 2018

Version 2.0.2 of the Apache XML Security for C++ has been released.

This patch corrects a [bug](#) that can cause crashes in upstream applications. It is similar to, but not the same as, the one that was patched in V2.0.1, and resulted from further review of the code by the project that contributes all of the current manpower to the project. Appreciation is extended to the [Shibboleth](#) Project team for this review.

August 2018

Version 2.0.1 of the Apache XML Security for C++ has been released.

This patch corrects a [bug](#) that can cause crashes in upstream applications.

June 2018

Version 2.1.2 of the Apache XML Security for Java library has been released.

Please see the [release notes](#) for more information.

Version 2.0.0 of the Apache XML Security for C++ has been released.

Please see the [release notes](#) for basic information on bugs addressed. As a major upgrade, this release includes a range of relative minor, but visible, changes to the API that are not explicitly noted there. There are no features of significance added in this version, merely some refactoring and removal of deprecated APIs.

January 2018

Versions 2.1.1 and 2.0.10 of the Apache XML Security for Java library have been released.

Please see the [release notes](#) for more information.

Apache XML Security for Java 2.1.0/2.0.9

Versions 2.1.0 and 2.0.9 of the Apache XML Security for Java library have been released.

Please see the [release notes](#) for more information.

Apache XML Security for Java 2.0.5

Version 2.0.5 of the Apache XML Security for Java library has been released.

Please see the [release notes](#) for more information.

Apache XML Security for Java 2.0.4

Versions 2.0.4 of the Apache XML Security for Java library has been released.

Please see the [release notes](#) for more information.

Apache XML Security for Java 2.0.3/1.5.8

Versions 2.0.3 and 1.5.8 of the Apache XML Security for Java library have been released. Security advisory [CVE-2014-8152](#) has been issued for versions 2.0.0, 2.0.1 and 2.0.2 of the library.

Please see the [release notes](#) for more information.

Apache XML Security for C++ 1.7.1

Security advisory [CVE-2013-2210](#) has been issued, affecting Apache XML-Security for C++ version 1.7.1. Version 1.7.2 of the Apache XML Security for C++ library has been released, addressing this issue.

Security advisory [CVE-2013-2172](#) has been issued for the Apache XML Security for Java project. Versions 1.4.8 and 1.5.5 have been released, fixing this issue.

Security advisories [CVE-2013-2153](#), [CVE-2013-2154](#), [CVE-2013-2155](#), and [CVE-2013-2156](#), affecting Apache XML-Security for C++ versions prior to 1.7.1, have been issued.

Version 1.7.1 of the Apache XML Security for C++ library has been released, addressing these issues.

Apache XML Security for Java 2.0.2

Versions 2.0.2 of the Apache XML Security for Java library has been released.

Please see the [release notes](#) for more information.

Apache XML Security for Java 2.0.1 and 1.5.7

Versions 2.0.1 and 1.5.7 of the Apache XML Security for Java library has been released.

Please see the [release notes](#) for more information.

Apache XML Security for Java 2.0.0

Version 2.0.0 of the Apache XML Security for Java library has been released.

Please see the [release notes](#) for more information.

Apache XML Security for Java 1.5.6

Version 1.5.6 of the Apache XML Security for Java library has been released.

Please see the [release notes](#) for more information.

This release fixes a new security advisory [CVE-2013-4517](#).

Apache XML Security for Java 1.5.5 and 1.4.8

Security advisory [CVE-2013-2172](#) has been issued for the Apache XML Security for Java project. Versions 1.4.8 and 1.5.5 have been released, fixing this issue.

Apache XML Security for Java 1.4.7

The Apache Santuario team are pleased to announce the release of version 1.4.7 of the Apache XML Security for Java library. This release fixes a problem with a missing KeyInfo Element when multiple elements are encrypted, as well as a number of other issues.

Please see the [release notes](#) for more information.

Apache XML Security for Java 1.5.4

Version 1.5.4 of the Apache XML Security for Java library has been released.

Please see the [release notes](#) for more information.

Apache XML Security for C++ 1.7.0

The Apache Santuario team are pleased to announce the release of version 1.7.0 of the Apache XML Security for C++ library. This release provides a few bug fixes and a partial implementation of XML Encryption 1.1 features, including AES-GCM encryption and some support for newer RSA-OAEP variants.

Apache XML Security for Java 1.5.3

Version 1.5.3 of the Apache XML Security for Java library has been released. This release features support for new XML Signature 1.1 KeyInfo extensions. It also fixes a number of bugs including a problem when message sizes are greater than 512 MB.

Please see the [release notes](#) for more information.

Apache XML Security for Java 1.5.2

Version 1.5.2 of the Apache XML Security for Java library has been released. The main feature of this release is that the default canonicalization algorithm for encryption has changed from inclusive with comments to a new canonicalization algorithm that preserves the physical representation of the element being encrypted. This change fixes a problem where an element might be decrypted to the wrong namespace.

Please see the [release notes](#) for more information.

Apache XML Security for C++ 1.6.1

The Apache Santuario team are pleased to announce the release of version 1.6.1 of the Apache XML Security for C++ library. This release provides bug fixes and addresses [CVE-2011-2516](#).

Apache XML Security for Java 1.5.1

Version 1.5.1 of the Apache XML Security for Java library has been released. This release fixes two important bugs - a bug in XMLSignatureInput when using a BufferedInputStream, as well as a bug which caused 1.5.0 to continue to require Xalan. It also contains some performance improvements for encryption and decryption.

Please see the [release notes](#) for more information.

Apache XML Security for Java 1.5.0

Version 1.5.0 of the Apache XML Security for Java library has been released. This is a major new release and is not binary compatible with the 1.4.x releases.

Please see the [release notes](#) for more information.

Apache XML Security for Java 1.4.6

The Apache Santuario team are pleased to announce the release of version 1.4.6 of the Apache XML Security for Java library. This release fixes a thread safety issue with XML Signature, a bug fix for the Canonical XML 1.1 algorithm, as well as a number of other bug fixes.

Please see the [release notes](#) for more information.

Apache XML Security for Java 1.4.5

The Apache Santuario team are pleased to announce the release of version 1.4.5 of the Apache XML Security for Java library. This release fixes a thread safety issue in the ResourceResolver, and a regression in signature generation for the Canonical XML 1.1 algorithm, as well as a number of other bug fixes.

Please see the [release notes](#) for more information.

Apache XML Security for C++ 1.6.0

The Apache Santuario team are pleased to announce the release of version 1.6.0 of the Apache XML Security for C++ library. This release provides many bug fixes and a partial implementation of XML Signature 1.1 features, including ECDSA signatures.

Apache XML Security for Java 1.4.4

The Apache Santuario team are pleased to announce the release of version 1.4.4 of the Apache XML Security for Java library. This release contains some enhancements to the resolver API's. It also fixes some longstanding issues with interned Strings, as well as a number of bug fixes.

Please see the [release notes](#) for more information.

Apache XML Security for Java 1.4.3

The Apache Santuario team are pleased to announce the release of version 1.4.3 of the XML Security Java library. This release provides many bug fixes and a fix for the recently announced HMAC vulnerability in the XML Signature specification. You should upgrade to this release as soon as possible.

Please see the [changelog](#) for more information.

Apache XML Security for C++ 1.5.1

The Apache Santuario team are pleased to announce the release of version 1.5.1 of the XML Security C++ library. This release provides some bug fixes and a fix for the recently announced HMAC vulnerability in the XML Signature specification.

Please see the [changelog](#) for more information.

Apache XML Security for C++ 1.5.0

Version 1.5.0 of the XML Security C++ library has been released. This release provides more bug fixes, partial support for Inclusive Canonicalization 1.1, and support for the Xerces 3.x official release and 32/64-bit portability APIs.

Please see the [changelog](#) for more information.

Apache XML Security for Java 1.4.2

Version 1.4.2 of the XML Security Java library has been released. This is mainly a bugfix release but also contains a few new enhancements including support for XML Canonicalization 1.1.

Please see the [changelog](#) for more information.

Apache XML Security for Java 1.4.1

Version 1.4.1 of the XML Security Java library has been released. This is a bugfix release that contains a major bugfix to the canonicalization engine introduced in the 1.4 release. It is recommended that 1.4 users upgrade to the new version as signatures containing non ascii characters created by this library are not according to the standard, and will be only validated by 1.4 library.

Please see the [changelog](#) for more information.

Apache XML Security for C++ 1.4.0

The Apache Santuario team are proud to announce the release of version 1.4.0 of the XML Security C++ library. This release provides more bug fixes, improved automake and RPM packaging, and better error reporting.

This version also provides initial support for Xerces 3.0. If you are building for the 3.0 library under Windows, you will need to change the Xerces library (in link includes) to xerces_3?.lib.

Please see the [changelog](#) for more information.

Apache XML Security for C++ 1.3.1

Version 1.3.1 of the XML Security C++ library has been released. This release contains some minor bug fixes and initial updates for Xerces 3.0. It also provides a new automake based build on *NIX. See the [changelog](#) for more information.

Apache XML Security for Java 1.4.0

Version 1.4 of the XML Security Java library has been released. The main changes for this version are:

- Implementation of the standard API JSR105
- Rewritten c14n that increase performance for signature with node-set transformations.
- Memory footprint reduction and several bugfixes

Refer to the [changelog](#) for more information.

Apache XML Security for C++ 1.3.0

Version 1.3 of the XML Security C++ library has been released. This release features performance improvements and a complete message set for XKMS. See the [changelog](#) for more information.

Apache XML Security for Java 1.3.0

Version 1.3 of the XML Security Java library has been released. This version provides :

- Better speed & memory utilization.
- Bug fixes.

See the [changelog](#) for more information.

Apache XML Security for C++ 1.2.1

Version 1.2.1 of the XML Security C++ library has been released. This minor release fixes versioning problems in the Windows project files. See the [changelog](#) for more information.

Apache XML Security for C++ 1.2.0

Version 1.2 of the XML Security C++ library has been released. This version includes a number of bug fixes, together with a beta release of code to process and generate XKMS messages. See the [changelog](#) for more information.

Apache XML Security for Java 1.2.1

Version 1.2.1 of the XML Security Java library has been released. This is a bugfix version, for more detail information see the [changelog](#).

Apache XML Security for Java 1.2.0

Version 1.2 of the XML Security Java library has been released. This version provides :

- Better speed & memory utilization.
- Easier JCE integration.

Apache XML Security for Java 1.1

Version 1.1 of the XML Security Java library has been released. This version provides :

- Beta implementation of XML Encryption
- Bug fixes to Signature implementation

Apache XML Security for C++ 1.1

Version 1.1 of the XML Security C++ library has been released. Supporting Xerces 2.5, 2.4 and 2.3 together with Xalan 1.6 and 1.7, this version provides :

- Beta implementation of XML Encryption
- Improved support for Windows Crypto API
- Bug fixes to Signature implementation

Apache XML Security for C++ 1.0

Version 1.00 of the XML Security C++ library is now released. This is the first stable release of the library. Functionality is still fairly basic, but all mandatory parts of the the DSIG standard are implemented.

This version supports Xerces 2.2 and 2.3 and Xalan 1.6.

Apache XML Security for C++ Beta 0.2

The Beta 0.20 of the XML Security C++ library has now been released. Features:

- Ability to use the Windows Crypto API as a crypto provider
- Several minor bug fixes in transforms and UNIX build process

Apache XML Security for Java 2.0.1 and 1.5.7