



# CVE-2013-2172

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2013-2172
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2013-08-20 22:55:00 UTC
<b>Updated</b>	2023-04-18 19:06:00 UTC
<b>Description</b>	jcp/xml/dsig/internal/dom/DOMCanonicalizationMethod.java in Apache Santuario XML Security for Java 1.4.x before 1.4.8 s

## Risk And Classification

**Problem Types:** CWE-310

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Santuario Xml Security For Java	1.4.7	All	All	All
Application	Apache	Santuario Xml Security For Java	1.5.0	All	All	All
Application	Apache	Santuario Xml Security For Java	1.5.1	All	All	All
Application	Apache	Santuario Xml Security For Java	1.5.2	All	All	All
Application	Apache	Santuario Xml Security For Java	1.5.3	All	All	All
Application	Apache	Santuario Xml Security For Java	1.5.4	All	All	All
Application	Apache	Xml Security For Java	1.4.7	All	All	All
Application	Apache	Xml Security For Java	1.5.0	All	All	All
Application	Apache	Xml Security For Java	1.5.1	All	All	All
Application	Apache	Xml Security For Java	1.5.2	All	All	All
Application	Apache	Xml Security For Java	1.5.3	All	All	All
Application	Apache	Xml Security For Java	1.5.4	All	All	All
Application	Apache	Xml Security For Java	1.4.7	All	All	All
Application	Apache	Xml Security For Java	1.5.0	All	All	All
Application	Apache	Xml Security For Java	1.5.1	All	All	All
Application	Apache	Xml Security For Java	1.5.2	All	All	All
Application	Apache	Xml Security For Java	1.5.3	All	All	All

Application	Apache	Xml Security For Java	1.5.4	All	All	All
-------------	--------	-----------------------	-------	-----	-----	-----

## References

### Reference

Red Hat Customer Portal

Red Hat Customer Portal

lists.apache.org/thread.html/r1c07a561426ec5579073046ad7f4207cdcef452bb3100aba...

Pony Mail!

VMSA-2014-0012 | United States

Red Hat Customer Portal

santuario.apache.org/secadv.data/CVE-2013-2172.txt.asc

Red Hat Customer Portal

Red Hat Customer Portal

USN-2028-1: Apache XML Security for Java vulnerability | Ubuntu

Red Hat Customer Portal

Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities

Red Hat Customer Portal

Red Hat Customer Portal

[Apache-SVN] Diff of /santuario/xml-security-java/branches/1.5.x-fixes/src/main/java/org/apache/jcp/xml/dsig/internal/dom/DOMCanonicalizati...

Apache Santuario XML Security for JAVA XML Signature CVE-2013-2172 Security Bypass Vulnerability

Pony Mail!

Security Advisory SA54019 - Apache XML Security Signature Spoofing Vulnerability - Secunia

Pony Mail!

Oracle Critical Patch Update - July 2014

Red Hat Customer Portal

Red Hat Customer Portal

SecurityFocus

94651

Debian -- Security Information -- DSA-3065-1 libxml-security-java

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)