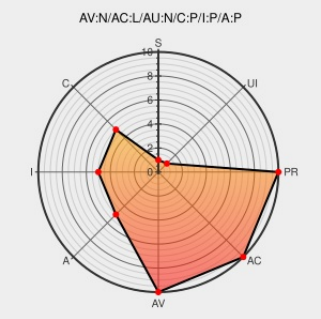
CVE-2013-2210

Published on: 08/20/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:43:00 AM UTC

CVE-2013-2210

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xml Security For C from Apache contain the following vulnerability:

Heap-based buffer overflow in the XML Signature Reference functionality in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.2 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via malformed XPointer expressions. NOTE: this is due to an incorrect fix for CVE-2013-2154.

CVE-2013-2210 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	Vendor Advisory, santuario.apache.org, text/plain	CONFIRM santuario.apache.org/secadv.data/CVE-2013-2210.txt
Pony Mail!	lists.apache.org, text/html	MLIST [santuario-commits] 20210917 svn commit: r1076843 - in /websites/production/santuario/content: cache/main.pageCache index.html javaindex.html secadv.data/CVE-2021-40690.txt.asc secadv.html
[R2] SecurityCenter 5.8.0 Fixes Multiple Third-Party Vulnerabilities - Security Advisory | Tenable®	www.tenable.com, text/html	CONFIRM www.tenable.com/security/tns-2018-15
Pony Mail!	lists.apache.org	MLIST [santuario-commits] 20190823 svn commit: r1049214 - in

	text/html	/websites/production/santuario/content: cache/main.pageCache download.html index.html javaindex.html javareleasenotes.html secadv.data/CVE-2019-12400.asc secadv.html
No Description Provided	archives.neohapsis.com Inactive Link Not Archived	FULLDISC 20130626 CVE-2013-2210
Debian -- Security Information -- DSA-2717-1 xml-security-c	www.debian.org Depreciated Link text/html	DEBIAN DSA-2717

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Xml Security For C	0.1.0	All	All	All
Application	Apache	Xml Security For C	0.2.0	All	All	All
Application	Apache	Xml Security For C	1.1.0	All	All	All
Application	Apache	Xml Security For C	1.2.0	All	All	All
Application	Apache	Xml Security For C	1.2.1	All	All	All
Application	Apache	Xml Security For C	1.3.0	All	All	All
Application	Apache	Xml Security For C	1.3.1	All	All	All
Application	Apache	Xml Security For C	1.4.0	All	All	All
Application	Apache	Xml Security For C	1.5.0	All	All	All
Application	Apache	Xml Security For C	1.5.1	All	All	All
Application	Apache	Xml Security For C	1.6.0	All	All	All
Application	Apache	Xml Security For C	1.6.1	All	All	All
Application	Apache	Xml Security For C	1.7.0	All	All	All
Application	Apache	Xml Security For C	All	All	All	All
Application	Apache	Xml Security For C	0.1.0	All	All	All
Application	Apache	Xml Security For C	0.2.0	All	All	All
Application	Apache	Xml Security For C	1.1.0	All	All	All
Application	Apache	Xml Security For C	1.2.0	All	All	All
Application	Apache	Xml Security For C	1.2.1	All	All	All
Application	Apache	Xml Security For C	1.3.0	All	All	All
Application	Apache	Xml Security For C	1.3.1	All	All	All

Application	Apache	Xml Security For C	1.4.0	All	All	All
Application	Apache	Xml Security For C	1.5.0	All	All	All
Application	Apache	Xml Security For C	1.5.1	All	All	All
Application	Apache	Xml Security For C	1.6.0	All	All	All
Application	Apache	Xml Security For C	1.6.1	All	All	All
Application	Apache	Xml Security For C	1.7.0	All	All	All
Application	Apache	Xml Security For C	0.1.0	All	All	All
Application	Apache	Xml Security For C	0.2.0	All	All	All
Application	Apache	Xml Security For C	1.1.0	All	All	All
Application	Apache	Xml Security For C	1.2.0	All	All	All
Application	Apache	Xml Security For C	1.2.1	All	All	All
Application	Apache	Xml Security For C	1.3.0	All	All	All
Application	Apache	Xml Security For C	1.3.1	All	All	All
Application	Apache	Xml Security For C	1.4.0	All	All	All
Application	Apache	Xml Security For C	1.5.0	All	All	All
Application	Apache	Xml Security For C	1.5.1	All	All	All
Application	Apache	Xml Security For C	1.6.0	All	All	All
Application	Apache	Xml Security For C	1.6.1	All	All	All
Application	Apache	Xml Security For C	1.7.0	All	All	All
Application	Apache	Xml Security For C	All	All	All	All

cpe:2.3:a:apache:xml_security_for_c++:0.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:0.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:1.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c++:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:0.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:0.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:0.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:0.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:1.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_c\+\+:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→