



CVE-2013-2156

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

Last Modified on: 09/17/2021 11:15:00 AM UTC

CVE-2013-2156

[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 Exclusive Canonicalization functionality (xsec/canon/XSECC14n20010315.cpp) in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PrefixList attribute.

CVE-2013-2156 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

[Apache-SVN] Revision 1493961

[Patch](#)
[svn.apache.org](#)
[text/html](#)

MISC svn.apache.org/viewvc?view=revision&revision=1493961

Debian -- Security Information --
DSA-2710-1 xml-security-c

[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

DEBIAN DSA-2710

[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

No Description Provided

[archives.neohapsis.com](#)

FULLDISC 20130617 Re: CVE-2013-2156: Apache Santuario C++ heap overflow vulnerability

[Inactive Link](#) **Not Archived**

	santuario.apache.org text/plain	 CONFIRM santuario.apache.org/secadv.data/CVE-2013-2156.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
Pony Mail!	lists.apache.org text/html	 MLIST [santuario-commits] 20190823 svn commit: r1049214 - in /websites/production/santuario/content: cache/main.pageCache download.html index.html javaindex.html javareleasenotes.html secadv.data/CVE-2019-12400.asc secadv.html
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	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	Package	Version	Severity	Impact	Exploitability	CVSS
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	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	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++:****:*:*:						
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\+\+: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_cplusplus: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\+\+:.*:.*:.*:.*:.*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)