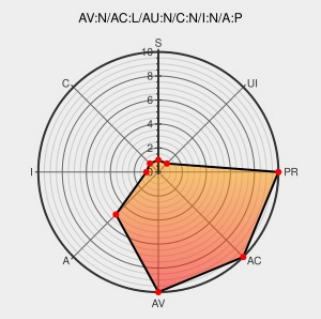
CVE-2013-2160

Published on: 08/19/2013 12:00:00 AM UTC

Last Modified on: 06/16/2021 12:15:00 PM UTC

CVE-2013-2160

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



Certain versions of Cxf from Apache contain the following vulnerability:

The streaming XML parser in Apache CXF 2.5.x before 2.5.10, 2.6.x before 2.6.7, and 2.7.x before 2.7.4 allows remote attackers to cause a denial of service (CPU and memory consumption) via crafted XML with a large number of (1) elements, (2) attributes, (3) nested constructs, and possibly other vectors.

CVE-2013-2160 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
[#WSTX-285] Add ability to restrict certain size limits of parsed XML - jira.codehaus.org	Patch, web.archive.org, text/html, Inactive Link, Not Archived	MISC jira.codehaus.org/browse/WSTX-285
Pony Mail!	lists.apache.org, text/html	MLIST [cxf-commits] 20200116 svn commit: r1055336 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2019-12423.txt.asc security-advisories.data/CVE-2019-17573.txt.asc security-advisories.html
Pony Mail!	lists.apache.org, text/html	MLIST [cxf-commits] 20210402 svn commit: r1073270 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2021-22696.txt.asc security-advisories.html
Pony Mail!	lists.apache.org, text/html	MLIST [cxf-commits] 20200319 svn commit: r1058035 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2019-17573.txt.asc security-advisories.html

[WSTX-287] Add more settings for various size restrictions - jira.codehaus.org	Patch web.archive.org text/html Inactive Link Not Archived	MISC jira.codehaus.org/browse/WSTX-287
Pony Mail!	lists.apache.org text/html	MLIST [cxf-commits] 20200401 svn commit: r1058573 - in /websites/production/cxf/content: cache/main.pageCache index.html security-advisories.data/CVE-2020-1954.txt.asc security-advisories.html
	Vendor Advisory cxf.apache.org text/plain	CONFIRM cxf.apache.org/security-advisories.data/CVE-2013-2160.txt.asc
Pony Mail!	lists.apache.org text/html	MLIST [cxf-commits] 20210616 svn commit: r1075801 - in /websites/production/cxf/content: cache/main.pageCache index.html security-advisories.data/CVE-2021-30468.txt.asc security-advisories.html
Pony Mail!	lists.apache.org text/html	MLIST [cxf-commits] 20201112 svn commit: r1067927 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2020-13954.txt.asc security-advisories.html
Red Hat Customer Portal	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1028
Bug 929197 – CVE-2013-2160 cxf, jbossws-cxf, apache-cxf: Multiple denial of service flaws in the StAX parser	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=929197
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1437

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Cxf	2.5.0	All	All	All
Application	Apache	Cxf	2.5.1	All	All	All
Application	Apache	Cxf	2.5.2	All	All	All
Application	Apache	Cxf	2.5.3	All	All	All
Application	Apache	Cxf	2.5.4	All	All	All
Application	Apache	Cxf	2.5.5	All	All	All
Application	Apache	Cxf	2.5.6	All	All	All
Application	Apache	Cxf	2.5.7	All	All	All

Application	Apache	Cxf	2.5.8	All	All	All
Application	Apache	Cxf	2.5.9	All	All	All
Application	Apache	Cxf	2.6.0	All	All	All
Application	Apache	Cxf	2.6.1	All	All	All
Application	Apache	Cxf	2.6.2	All	All	All
Application	Apache	Cxf	2.6.3	All	All	All
Application	Apache	Cxf	2.6.4	All	All	All
Application	Apache	Cxf	2.6.5	All	All	All
Application	Apache	Cxf	2.6.6	All	All	All
Application	Apache	Cxf	2.7.0	All	All	All
Application	Apache	Cxf	2.7.1	All	All	All
Application	Apache	Cxf	2.7.2	All	All	All
Application	Apache	Cxf	2.7.3	All	All	All
Application	Apache	Cxf	2.5.0	All	All	All
Application	Apache	Cxf	2.5.1	All	All	All
Application	Apache	Cxf	2.5.2	All	All	All
Application	Apache	Cxf	2.5.3	All	All	All
Application	Apache	Cxf	2.5.4	All	All	All
Application	Apache	Cxf	2.5.5	All	All	All
Application	Apache	Cxf	2.5.6	All	All	All
Application	Apache	Cxf	2.5.7	All	All	All
Application	Apache	Cxf	2.5.8	All	All	All
Application	Apache	Cxf	2.5.9	All	All	All
Application	Apache	Cxf	2.6.0	All	All	All
Application	Apache	Cxf	2.6.1	All	All	All
Application	Apache	Cxf	2.6.2	All	All	All
Application	Apache	Cxf	2.6.3	All	All	All
Application	Apache	Cxf	2.6.4	All	All	All
Application	Apache	Cxf	2.6.5	All	All	All
Application	Apache	Cxf	2.6.6	All	All	All
Application	Apache	Cxf	2.7.0	All	All	All
Application	Apache	Cxf	2.7.1	All	All	All
Application	Apache	Cxf	2.7.2	All	All	All
Application	Apache	Cxf	2.7.3	All	All	All

cpe:2.3:a:apache:cxf:2.5.0:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.1:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.2:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.3:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.4:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.5:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.6:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.7:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.8:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.9:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.0:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.1:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.2:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.3:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.4:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.5:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.6:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.7.0:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.7.1:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.7.2:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.7.3:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.0:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.1:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.2:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.3:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.4:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.5:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.6:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.7:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.8:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.5.9:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.0:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.1:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.2:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.3:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.4:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.5:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.6.6:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.7.0:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.7.1:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.7.2:*:*:*:*:*:*:*

cpe:2.3:a:apache:cxf:2.7.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→