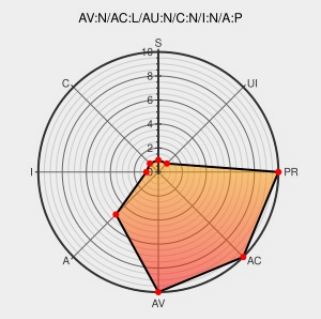
CVE-2004-1575

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1575

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



Certain versions of Xerces-c from Apache contain the following vulnerability:

The XML parser in Xerces-C++ 2.5.0 allows remote attackers to cause a denial of service (CPU consumption) via XML attributes in a crafted XML document.

CVE-2004-1575 has been assigned by cve@mitre.org 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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF xercescplusplus-xml-parser-dos(17575)
Secunia - Advisories - Xerces-C++ XML Parser Denial of Service Vulnerability	Patch web.archive.org text/html	SECUNIA 12715
Xerces C++ Duplicated Attributes XML Parsing Denial Of Service Vulnerability	Patch cve.report (archive) text/html	BID 11312
'Security advisory - Xerces-C++ 2.5.0: Attribute blowup' - MARC	marc.info text/html	BUGTRAQ 20041002 Security advisory - Xerces-C++ 2.5.0: Attribute blowup

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	Xerces-c	2.5.0	All	All	All
Application	Apache	Xerces-c	2.5.0	All	All	All
Application	Apache	Xerces-c	2.5.0	All	All	All

cpe:2.3:a:apache:xerces-c++:2.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xerces-c\+\+:2.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xerces-c\+\+:2.5.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→