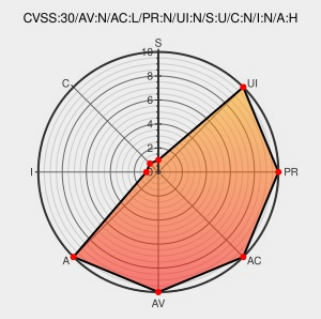
CVE-2012-0880

Published on: 08/08/2017 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:13 AM UTC

CVE-2012-0880

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



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

Apache Xerces-C++ allows remote attackers to cause a denial of service (CPU consumption) via a crafted message sent to an XML service that causes hash table collisions.

CVE-2012-0880 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
787103 – (CVE-2012-0880) CVE-2012-0880 xml: xerces-c hash table collisions CPU usage DoS (oCERT-2011-003)	Issue Tracking, Third Party Advisory, VDB Entry, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=787103

oss-sec: Summer bug cleaning - some Hash DoS stuff	Mailing List Third Party Advisory seclists.org text/html	MLIST [oss-security] 20140708 Summer bug cleaning - some Hash DoS stuff

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→