CVE-2009-1885

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-1885
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-11 18:30:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	Stack consumption vulnerability in validators/DTD/DTDScanner.cpp in Apache Xerces C++ 2.7.0 and 2.8.0 allows context-c

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Xerces-c	2.7.0	All	All	All
Application	Apache	Xerces-c	2.8.0	All	All	All
Application	Apache	Xerces-c	2.7.0	All	All	All
Application	Apache	Xerces-c	2.8.0	All	All	All
Application	Apache	Xerces-c	2.7.0	All	All	All
Application	Apache	Xerces-c	2.8.0	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 10 Update: xerces-c-2.8.0-5.fc10	FEDORA	www.redhat.com
Codenomicon Labs | XML Security and Fuzzing	MISC	www.codenomic
[SECURITY] Fedora 11 Update: xerces-c-2.8.0-5.fc11	FEDORA	www.redhat.com
IBM X-Force Exchange	XF	exchange.xforce
CERT-FI - CERT-FI Advisory on XML libraries	MISC	www.cert.fi
svn.apache.org/viewvc/xerces/c/trunk/src/xercesc/validators/DTD/DTDScanner.cpp	CONFIRM	svn.apache.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Bug 515515 – CVE-2009-1885 xerces-c, xerces-c27: Stack overflow when parsing recursive XML structures	CONFIRM	bugzilla.redhat.c

Xerces-C++ Nested DTD Structure XML Parsing Remote Denial of Service Vulnerability	BID	www.securityfoc
Xerces-C++ XML DTD Structures Parsing Denial of Service - Secunia.com	SECUNIA	secunia.com
XML flaw threatens apps built with Sun, Apache, Python libraries - Network World	MISC	www.networkwo
Security Advisories | Mandriva Linux	MANDRIVA	www.mandriva.c
[SECURITY] Fedora 11 Update: xerces-c27-2.7.0-8.fc11	FEDORA	www.redhat.com
[Apache-SVN] Revision 781488	CONFIRM	svn.apache.org
[SECURITY] Fedora 10 Update: xerces-c27-2.7.0-8.fc10	FEDORA	www.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-08-12	Tomas Hoger	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com

There are currently no legacy QID mappings associated with this CVE.