CVE-2007-6284

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2007-6284
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-12 02:46:00 UTC
Updated	2023-02-13 02:18:00 UTC
Description	The xmlCurrentChar function in libxml2 before 2.6.31 allows context-dependent attackers to cause a denial of service (infini

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	All	alpha	All
Operating System	Debian	Debian Linux	3.1	All	amd64	All
Operating System	Debian	Debian Linux	3.1	All	arm	All
Operating System	Debian	Debian Linux	3.1	All	hppa	All
Operating System	Debian	Debian Linux	3.1	All	ia-32	All
Operating System	Debian	Debian Linux	3.1	All	ia-64	All
Operating System	Debian	Debian Linux	3.1	All	m68k	All
Operating System	Debian	Debian Linux	3.1	All	mips	All
Operating System	Debian	Debian Linux	3.1	All	mipsel	All
Operating System	Debian	Debian Linux	3.1	All	ppc	All
Operating System	Debian	Debian Linux	3.1	All	s-390	All
Operating System	Debian	Debian Linux	3.1	All	sparc	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	alpha	All
Operating System	Debian	Debian Linux	4.0	All	amd64	All
Operating System	Debian	Debian Linux	4.0	All	arm	All

Operating System	Debian	Debian Linux	4.0	All	hppa	All
Operating System	Debian	Debian Linux	4.0	All	ia-32	All
Operating System	Debian	Debian Linux	4.0	All	ia-64	All
Operating System	Debian	Debian Linux	4.0	All	m68k	All
Operating System	Debian	Debian Linux	4.0	All	mips	All
Operating System	Debian	Debian Linux	4.0	All	mipsel	All
Operating System	Debian	Debian Linux	4.0	All	powerpc	All
Operating System	Debian	Debian Linux	4.0	All	s-390	All
Operating System	Debian	Debian Linux	4.0	All	sparc	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	All	alpha	All
Operating System	Debian	Debian Linux	3.1	All	amd64	All
Operating System	Debian	Debian Linux	3.1	All	arm	All
Operating System	Debian	Debian Linux	3.1	All	hppa	All
Operating System	Debian	Debian Linux	3.1	All	ia-32	All
Operating System	Debian	Debian Linux	3.1	All	ia-64	All
Operating System	Debian	Debian Linux	3.1	All	m68k	All
Operating System	Debian	Debian Linux	3.1	All	mips	All
Operating System	Debian	Debian Linux	3.1	All	mipsel	All
Operating System	Debian	Debian Linux	3.1	All	ppc	All
Operating System	Debian	Debian Linux	3.1	All	s-390	All
Operating System	Debian	Debian Linux	3.1	All	sparc	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	alpha	All
Operating System	Debian	Debian Linux	4.0	All	amd64	All
Operating System	Debian	Debian Linux	4.0	All	arm	All
Operating System	Debian	Debian Linux	4.0	All	hppa	All
Operating System	Debian	Debian Linux	4.0	All	ia-32	All
Operating System	Debian	Debian Linux	4.0	All	ia-64	All
Operating System	Debian	Debian Linux	4.0	All	m68k	All
Operating System	Debian	Debian Linux	4.0	All	mips	All
Operating System	Debian	Debian Linux	4.0	All	mipsel	All
Operating System	Debian	Debian Linux	4.0	All	powerpc	All
Operating System	Debian	Debian Linux	4.0	All	s-390	All
Operating System	Debian	Debian Linux	4.0	All	sparc	All

Operating System	Mandrakesoft	Mandrake Linux	2007	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2007	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	2007.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2007.1	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	2008.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2008.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	2007	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2007	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	2007.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2007.1	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	2008.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2008.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	x86_64	All
Operating System	Redhat	Fedora	7	All	All	All
Operating System	Redhat	Fedora	8	All	All	All
Operating System	Redhat	Fedora	7	All	All	All
Operating System	Redhat	Fedora	8	All	All	All

References

Reference	Source	Link
Repository / Oval Repository	OVAL	oval.cisecur
Apple iPhone / iPod touch Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.con
ASA-2008-047 (SUN 201514, Previous ID: 103201)	CONFIRM	support.ava
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.con
SecurityFocus	BUGTRAQ	www.securit
Gentoo Bug 202628 - dev-libs/libxml2 < 2.6.30-r1 xmlCurrentChar() UTF-8 DoS (CVE-2007-6284)	CONFIRM	bugs.gentoo
rPath update for libxml2 - Advisories - Secunia	SECUNIA	secunia.con
USN-569-1: libxml2 vulnerability | Ubuntu security notices	UBUNTU	usn.ubuntu.
Sun Solaris Libxml2 UTF-8 Parsing Denial of Service - Advisories - Secunia	SECUNIA	secunia.con

Debian -- Security Information -- DSA-1461-1 libxml2	DEBIAN	www.debian
SecurityFocus	BUGTRAQ	www.securit
Avaya Products Libxml2 UTF-8 Parsing Denial of Service - Advisories - Secunia	SECUNIA	secunia.com
Red Hat Customer Portal	MISC	access.redh
Repository / Oval Repository	OVAL	oval.cisecur
[SECURITY] Fedora 7 Update: libxml2-2.6.31-1.fc7	FEDORA	www.redhat
Fedora update for libxml2 - Secunia.com	SECUNIA	secunia.com
Ubuntu update for libxml2 - Advisories - Secunia	SECUNIA	secunia.com
Releases	CONFIRM	www.xmlsof
Gentoo Linux Documentation -- libxml2: Denial of Service	GENTOO	security.gen
Libxml2 UTF-8 Validation Flaw Lets Remote Users Deny Service - SecurityTracker	SECTRACK	securitytrack
425927 – (CVE-2007-6284) CVE-2007-6284 libxml2: infinite loop in UTF-8 decoding	MISC	bugzilla.redh
Red Hat update for libxml2 - Advisories - Secunia	SECUNIA	secunia.com
APPLE-SA-2008-07-11 iPhone 2.0 and iPod touch 2.0	APPLE	lists.apple.c
[Security-announce] VMSA-2008-0006 Updated libxml2 service console package	MLIST	lists.vmware
Support	REDHAT	www.redhat
[SECURITY] Fedora 8 Update: libxml2-2.6.31-1.fc8	FEDORA	www.redhat
Webmail | OVH- OVH	VUPEN	www.vupen
Webmail | OVH- OVH	VUPEN	www.vupen
Security Announcement	SUSE	www.novell.
[xml] Security flaw affecting all previous libxml2 releases	MLIST	mail.gnome
access.redhat.com | CVE-2007-6284	MISC	access.redh
Support / Security / Advisories / / MDVSA-2008:010 | Mandriva	MANDRIVA	www.mandr
103201	SUNALERT	sunsolve.su
ASA-2008-050 (RHSA-2008-0032)	CONFIRM	support.ava
201514	SUNALERT	sunsolve.su
Gentoo update for libxml2 - Advisories - Secunia	SECUNIA	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen
Debian update for libxml2 - Secunia.com	SECUNIA	secunia.com
VMware ESX Server update for libxml2 - Advisories - Secunia	SECUNIA	secunia.com
Webmail | OVH- OVH	VUPEN	www.vupen
libxml2 'xmlCurrentChar()' UTF-8 Parsing Remote Denial of Service Vulnerability	BID	www.securit
Mandriva update for libxml2 - Secunia.com	SECUNIA	secunia.com
issues.rpath.com/browse/RPL-2121	CONFIRM	issues.rpath
Libxml2 UTF-8 Parsing Denial of Service Vulnerability - Advisories - Secunia	SECUNIA	secunia.com

CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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