CVE-2009-3560

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

Summary

CVE	CVE-2009-3560
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-12-04 21:30:00 UTC
Updated	2023-11-07 02:04:00 UTC
Description	The big2_toUtf8 function in lib/xmltok.c in libexpat in Expat 2.0.1, as used in the XML-Twig module for Perl, allows context-d

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Application	James Clark	Expat	2.0.1	All	All	All
Application	James Clark	Expat	2.0.1	All	All	All
Application	Libexpat Project	Libexpat	2.0.1	All	All	All
Application	Xmltwig	Xml-twig For Perl	All	All	All	All
Application	Xmltwig	Xml-twig For Perl	All	All	All	All

References

Reference	Source
About Secunia Research | Flexera	SECUNIA
[SECURITY] Fedora 10 Update: expat-2.0.1-8.fc10	FEDORA
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:014	SUSE
Pony Mail!	
[Expat-bugs] [expat-Bugs-2894085] expat: buffer over-read and crash in big2_toUtf8()	MLIST
Pony Mail!	
Pony Mail!	MLIST
Pony Mail!	MLIST

Pony Mail!	
Pony Mail!	MLIST
USN-890-1: Expat vulnerabilities | Ubuntu	UBUNTU
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Pony Mail!	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Support / Security / Advisories / / MDVSA-2009:316 | Mandriva	MANDRIVA
Pony Mail!	
Pony Mail!	MLIST
Pony Mail!	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Pony Mail!	
Pony Mail!	
Pony Mail!	MLIST
Pony Mail!	
Pony Mail!	MLIST
Pony Mail!	
Pony Mail!	
Pony Mail!	
Red Hat Customer Portal	REDHAT
Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	
VMware ESX Server Multiple Vulnerabilities - Advisories - Community	SECUNIA
CVS Info for project expat	CONFIRM
Pony Mail!	
Pony Mail!	MLIST
About Secunia Research | Flexera	SECUNIA
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:012	SUSE
[SECURITY] Fedora 11 Update: expat-2.0.1-8.fc11	FEDORA
Repository / Oval Repository	OVAL
Pony Mail!	
Security Tracker Archive expat Buffer Overflow in XML_GetBuffer() Lets Users Run Service	SECTRACK

SecurityTracker.com Archives - expat Buffer Over-read in big2_toUtf8() Lets Users Deny Service	SECTRACK
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE
Pony Mail!	
Pony Mail!	
Repository / Oval Repository	OVAL
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:011	SUSE
Ubuntu update for cmake - Advisories - Community	SECUNIA
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:001	SUSE
VMware vMA Update for Multiple Packages - Advisories - Community	SECUNIA
Pony Mail!	MLIST
USN-890-6: CMake vulnerabilities | Ubuntu	UBUNTU
Pony Mail!	MLIST
273630	SUNALERT
CVS Info for project expat	CONFIRM
Bug 533174 – CVE-2009-3560 expat: buffer over-read and crash in big2_toUtf8() on XML with malformed UTF-8 sequences	CONFIRM
Debian -- Security Information -- DSA-1953-1 expat	DEBIAN
Pony Mail!	
Pony Mail!	MLIST
'[security bulletin] HPSBUX02645 SSRT100387 rev.1 - HP-UX Apache Web Server, Remote Information Discl' - MARC	HP
Pony Mail!	
[Security-announce] VMSA-2010-0004 ESX Service Console and vMA third party updates	MLIST
Pony Mail!	
Ubuntu update for expat - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Pony Mail!	MLIST
Repository / Oval Repository	OVAL
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:013	SUSE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Apache APR-util Multiple Denial of Service Vulnerabilities - Advisories - Community	SECUNIA
Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	MLIST
VMware ESX Server 4 Multiple Vulnerabilities - Advisories - Community	SECUNIA
Expat XML Parsing Remote Denial of Service Vulnerability	BID
[SECURITY] Fedora 12 Update: expat-2.0.1-8.fc12	FEDORA
Pony Mail!	MLIST
Pony Mail!	MITRE

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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