CVE-2009-0689

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2009-0689
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-01 13:00:00 UTC
Updated	2018-11-02 10:29:00 UTC
Description	Array index error in the (1) dtoa implementation in dtoa.c (aka pdtoa.c) and the (2) gdtoa (aka new dtoa) implementation in

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	6.4	All	All	All
Operating System	Freebsd	Freebsd	6.4	release	All	All
Operating System	Freebsd	Freebsd	6.4	release_p2	All	All
Operating System	Freebsd	Freebsd	6.4	release_p3	All	All
Operating System	Freebsd	Freebsd	6.4	release_p4	All	All
Operating System	Freebsd	Freebsd	6.4	release_p5	All	All
Operating System	Freebsd	Freebsd	6.4	stable	All	All
Operating System	Freebsd	Freebsd	7.2	All	All	All
Operating System	Freebsd	Freebsd	7.2	pre-release	All	All
Operating System	Freebsd	Freebsd	7.2	stable	All	All
Operating System	Freebsd	Freebsd	6.4	All	All	All
Operating System	Freebsd	Freebsd	6.4	release	All	All
Operating System	Freebsd	Freebsd	6.4	release_p2	All	All
Operating System	Freebsd	Freebsd	6.4	release_p3	All	All
Operating System	Freebsd	Freebsd	6.4	release_p4	All	All
Operating System	Freebsd	Freebsd	6.4	release_p5	All	All
Operating System	Freebsd	Freebsd	6.4	stable	All	All

Operating System	Freebsd	Freebsd	7.2	All	All	All
Operating System	Freebsd	Freebsd	7.2	pre-release	All	All
Operating System	Freebsd	Freebsd	7.2	stable	All	All
Application	K-meleon Project	K-meleon	1.5.3	All	All	All
Application	K-meleon Project	K-meleon	1.5.3	All	All	All
Application	Mozilla	Firefox	3.0.1	All	All	All
Application	Mozilla	Firefox	3.0.10	All	All	All
Application	Mozilla	Firefox	3.0.11	All	All	All
Application	Mozilla	Firefox	3.0.12	All	All	All
Application	Mozilla	Firefox	3.0.13	All	All	All
Application	Mozilla	Firefox	3.0.14	All	All	All
Application	Mozilla	Firefox	3.0.2	All	All	All
Application	Mozilla	Firefox	3.0.3	All	All	All
Application	Mozilla	Firefox	3.0.4	All	All	All
Application	Mozilla	Firefox	3.0.5	All	All	All
Application	Mozilla	Firefox	3.0.6	All	All	All
Application	Mozilla	Firefox	3.0.7	All	All	All
Application	Mozilla	Firefox	3.0.8	All	All	All
Application	Mozilla	Firefox	3.0.9	All	All	All
Application	Mozilla	Firefox	3.5	All	All	All
Application	Mozilla	Firefox	3.5.1	All	All	All
Application	Mozilla	Firefox	3.5.2	All	All	All
Application	Mozilla	Firefox	3.5.3	All	All	All
Application	Mozilla	Firefox	3.0.1	All	All	All
Application	Mozilla	Firefox	3.0.10	All	All	All
Application	Mozilla	Firefox	3.0.11	All	All	All
Application	Mozilla	Firefox	3.0.12	All	All	All
Application	Mozilla	Firefox	3.0.13	All	All	All
Application	Mozilla	Firefox	3.0.14	All	All	All
Application	Mozilla	Firefox	3.0.2	All	All	All
Application	Mozilla	Firefox	3.0.3	All	All	All
Application	Mozilla	Firefox	3.0.4	All	All	All
Application	Mozilla	Firefox	3.0.5	All	All	All
Application	Mozilla	Firefox	3.0.6	All	All	All
Application	Mozilla	Firefox	3.0.7	All	All	All

Application	Mozilla	Firefox	3.0.8	All	All	All
Application	Mozilla	Firefox	3.0.9	All	All	All
Application	Mozilla	Firefox	3.5	All	All	All
Application	Mozilla	Firefox	3.5.1	All	All	All
Application	Mozilla	Firefox	3.5.2	All	All	All
Application	Mozilla	Firefox	3.5.3	All	All	All
Application	Mozilla	Seamonkey	1.1.8	All	All	All
Application	Mozilla	Seamonkey	1.1.8	All	All	All
Operating System	Netbsd	Netbsd	5.0	All	All	All
Operating System	Netbsd	Netbsd	5.0	All	All	All
Operating System	Openbsd	Openbsd	4.5	All	All	All
Operating System	Openbsd	Openbsd	4.5	All	All	All

References

Reference	Source
272909	SUNAL
SecurityFocus	BUGTF
Opera 10.01 Remote Array Overrun (Arbitrary code execution) (Research Advisory) - SecurityReason.com	SREAS
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
CVS log for src/lib/libc/gdtoa/gdtoaimp.h	CONFI
Mozilla Thunderbird Floating Point Parsing Memory Corruption - Secunia Advisories - Vulnerability Information - Secunia.com	SECUN
CVS log for src/lib/libc/gdtoa/misc.c	CONFI
Multiple BSD printf(1) and multiple dtoa/*printf(3) vulnerabilities (Research Advisory) - SecurityReason.com	SREAS
Advisory: Heap buffer overflow in string to number conversion - Opera Knowledge Base	CONFI
Webmail - OVH	VUPEN
Opera Floating Point Number Processing Memory Corruption - Secunia Advisories - Vulnerability Information - Secunia.com	SECUN
SecurityTracker.com Archives - libc gdtoa Array Overrun May Let Remote or Local Users Execute Arbitrary Code	SECTR
Apple Mac OS X "strtod()" Floating Point Parsing Memory Corruption - Secunia Advisories - Vulnerability Information - Secunia.com	SECUN
Thunderbird 2.0.0.23 (lib) Remote Array Overrun (Arbitrary code execution) (Research Advisory) - SecurityReason.com	SREAS
Support / Security / Advisories / / MDVSA-2009:330 | Mandriva	MANDR
USN-915-1: Thunderbird vulnerabilities | Ubuntu	UBUNT
Sunbird Floating Point Parsing Memory Corruption Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUN
Webmail - OVH	VUPEN
SecurityFocus	BUGTF
Red Hat Customer Portal	REDHA
Repository / Oval Repository	OVAL

Camino 1.6.10 Remote Array Overrun (Arbitrary code execution) (Research Advisory) - SecurityReason.com	SREAS
Support	REDHA
SecurityFocus	BUGTF
Sunbird 0.9 Array Overrun (code execution) (Research Advisory) - SecurityReason.com	SREAS
About the security content of iOS 4	CONFI
SecurityFocus	BUGTF
Ubuntu update for thunderbird - Advisories - Community	SECUN
Support | Red Hat	REDHA
Support	REDHA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3	APPLE
Flock 2.5.2 Remote Array Overrun (Arbitrary code execution) (Research Advisory) - SecurityReason.com	SREAS
MacOS X 10.5/10.6 libc/strtod(3) buffer overflow (Research Advisory) - SecurityReason.com	SREAS
APPLE-SA-2010-06-21-1 iOS 4	APPLE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
SeaMonkey 1.1.8 Remote Array Overrun (Arbitrary code execution) (Research Advisory) - SecurityReason.com	SREAS
About Secunia Research | Flexera	MISC
MFSA 2009-59: Heap buffer overflow in string to number conversion	CONFI
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:018	SUSE
K-Meleon 1.5.3 Remote Array Overrun (Arbitrary code execution) (Research Advisory) - SecurityReason.com	SREAS
Multiple Vendors libc/gdtoa printf(3) Array Overrun (Research Advisory) - SecurityReason.com	SREAS
Mozilla SeaMonkey Multiple Vulnerabilities - Advisories - Community	SECUN
Support / Security / Advisories / / MDVSA-2009:294 | Mandriva	MANDR
Red Hat Customer Portal	REDHA
Repository / Oval Repository	OVAL
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:013	SUSE
516862 – Array indexing error in js/src/dtoa.c's Balloc() leads to floating point memory vulnerability (SA36711)	CONFI
[SECURITY] [DLA 1564-1] mono security update	MLIST
Multiple BSD Distributions 'gdtoa/misc.c' Memory Corruption Vulnerability	BID
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	CONFI
516396 – (CVE-2009-0689) Array indexing error in NSPR's Balloc() leads to floating point memory vulnerability (SA36711)	CONFI
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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