CVE-2004-0718

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

Summary

CVE	CVE-2004-0718
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-07-27 04:00:00 UTC
Updated	2017-10-11 01:29:00 UTC
Description	The (1) Mozilla 1.6, (2) Firebird 0.7, (3) Firefox 0.8, and (4) Netscape 7.1 web browsers do not properly prevent a frame in c

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Firebirdsql	Firebird	0.7	All	All	All
Application	Firebirdsql	Firebird	0.7	All	All	All
Application	Mozilla	Mozilla	1.6	All	All	All
Application	Mozilla	Mozilla	1.6	All	All	All
Application	Netscape	Navigator	7.1	All	All	All
Application	Netscape	Navigator	7.1	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-810-1 mozilla	DEBIAN	www.debian.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.co
Secunia - Advisories - Multiple Browsers Frame Injection Vulnerability	SECUNIA	secunia.com
SCOSA-2005.49	SCO	ftp.sco.com
'[FLSA-2004:2089] Updated mozilla packages fix security vulnerabilities' - MARC	FEDORA	marc.info
SCO OpenServer Release 5.0.7 Maintenance Pack 4 Released - Multiple Vulnerabilities Fixed	BID	www.securityfocus.com
Security Announcement	SUSE	www.novell.com

246448 – can spoof framed sites by changing frame contents	CONFIRM	bugzilla.mozilla.org
redhat.com | Red Hat Support	REDHAT	www.redhat.com
Secunia - Multiple Browsers Frame Injection Vulnerability Test	MISC	secunia.com
Advisories - Mandriva	MANDRAKE	www.mandriva.com
Debian -- Security Information -- DSA-777-1 mozilla	DEBIAN	www.debian.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
CVE Program record	CVE.ORG	www.cve.org
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**