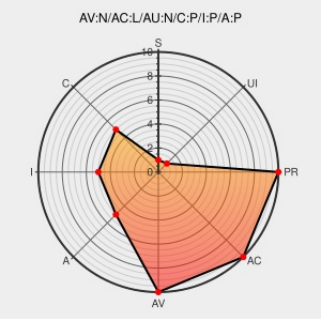
CVE-2005-2701

Published on: 09/23/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:26 AM UTC

CVE-2005-2701

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Firefox from Mozilla contain the following vulnerability:

Heap-based buffer overflow in Firefox before 1.0.7 and Mozilla Suite before 1.7.12 allows remote attackers to execute arbitrary code via an XBM image file that ends in a large number of spaces instead of the expected end tag.

CVE-2005-2701 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[FLSA-2006:168375] Updated mozilla packages fix security issues	www.redhat.com text/html	FEDORA FLSA-2006:168375
Advisories - Mandriva	www.mandriva.com text/html	MANDRIVA MDKSA-2005:174
Secunia - Advisories - Debian update for mozilla-thunderbird	web.archive.org text/html	SECUNIA 17284
	ftp.sco.com text/plain	SCO SCOSA-2005.49
Secunia - Advisories - Mozilla Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 16917
SCO OpenServer Release 5.0.7 Maintenance Pack 4 Released - Multiple Vulnerabilities Fixed	cve.report (archive) text/html	BID 15495

Debian -- Security Information -- DSA-866-1 mozilla	www.debian.org Depreciated Link text/html	DEBIAN DSA-866
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mozilla-xbm-bo(22373)
rhn.redhat.com | Red Hat Support	Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2005:785
Debian -- Security Information -- DSA-868-1 mozilla-thunderbird	www.debian.org Depreciated Link text/html	DEBIAN DSA-868
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1480
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9323
SecurityTracker.com Archives - Mozilla Firefox Integer/Buffer Overflows, Spoofing Bugs, and Access Control Errors Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1014954
Secunia - Advisories - Debian update for mozilla	web.archive.org text/html	SECUNIA 17263
Advisories - Mandriva	www.mandriva.com text/html	MANDRIVA MDKSA-2005:169
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:789
Secunia - Advisories - Firefox Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 16911
MFSA 2005-58 Firefox 1.0.7 / Mozilla Suite 1.7.12 Vulnerability Fixes	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/mfsa2005-58.html
Advisories - Mandriva	www.mandriva.com text/html	MANDRIVA MDKSA-2005:170
Secunia - Advisories - Debian update for mozilla-firefox	web.archive.org text/html	SECUNIA 17026
Secunia - Advisories - SUSE update for mozilla/MozillaFirefox	web.archive.org text/html	SECUNIA 17014
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2005:058
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 19643
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-1824
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	web.archive.org text/html	SECUNIA 16977
Secunia - Advisories - Ubuntu update for mozilla-thunderbird	web.archive.org text/html	SECUNIA 17149
usn/usn-200-1 - Ubuntu Linux	www.ubuntu.com	UBUNTU USN-200-1

usn/usn-200-1 - Ubuntu Linux	www.ubuntu.com text/html	UBUNTU USN-200-1
Debian -- Security Information -- DSA-838-1 mozilla-firefox	www.debian.org Depreciated Link text/html	DEBIAN DSA-838
Mozilla Browser/Firefox XBM Image Processing Heap Overflow Vulnerability	cve.report (archive) text/html	BID 14916

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	1.0	All	All	All
Application	Mozilla	Firefox	1.0.1	All	All	All
Application	Mozilla	Firefox	1.0.2	All	All	All
Application	Mozilla	Firefox	1.0.3	All	All	All
Application	Mozilla	Firefox	1.0.4	All	All	All
Application	Mozilla	Firefox	1.0.5	All	All	All
Application	Mozilla	Firefox	1.0	All	All	All
Application	Mozilla	Firefox	1.0.1	All	All	All
Application	Mozilla	Firefox	1.0.2	All	All	All
Application	Mozilla	Firefox	1.0.3	All	All	All
Application	Mozilla	Firefox	1.0.4	All	All	All
Application	Mozilla	Firefox	1.0.5	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Mozilla Suite	1.7.10	All	All	All
Application	Mozilla	Mozilla Suite	1.7.6	All	All	All
Application	Mozilla	Mozilla Suite	1.7.7	All	All	All
Application	Mozilla	Mozilla Suite	1.7.8	All	All	All
Application	Mozilla	Mozilla Suite	1.7.10	All	All	All
Application	Mozilla	Mozilla Suite	1.7.6	All	All	All
Application	Mozilla	Mozilla Suite	1.7.7	All	All	All
Application	Mozilla	Mozilla Suite	1.7.8	All	All	All
Application	Mozilla	Mozilla Suite	All	All	All	All

cpe:2.3:a:mozilla:firefox:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:mozilla_suite:1.7.10:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:mozilla_suite:1.7.6:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:mozilla_suite:1.7.7:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:mozilla_suite:1.7.8:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:mozilla_suite:1.7.10:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:mozilla_suite:1.7.6:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:mozilla_suite:1.7.7:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:mozilla_suite:1.7.8:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:mozilla_suite:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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