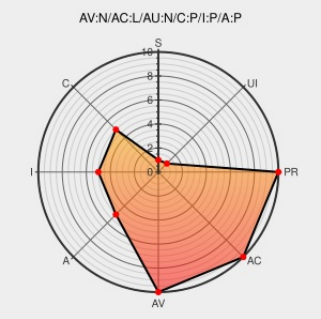
CVE-2005-2871

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

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

CVE-2005-2871

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



Certain versions of Firefox from Mozilla contain the following vulnerability:

Buffer overflow in the International Domain Name (IDN) support in Mozilla Firefox 1.0.6 and earlier, and Netscape 8.0.3.3 and 7.2, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a hostname with all "soft" hyphens (character 0xAD), which is not properly handled by the NormalizeIDN call in nsStandardURL::BuildNormalizedSpec.

CVE-2005-2871 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
Gentoo Linux Documentation -- Mozilla Suite, Mozilla Firefox: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-200509-11
Advisories - Mandriva	www.mandriva.com text/html	MANDRIVA MDKSA-2005:174
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 19255
Secunia - Advisories - Debian update for mozilla-	web.archive.org	SECUNIA 17284

thunderbird	text/html	
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CIAC P-303
Secunia - Advisories - Firefox IDN URL Domain Name Buffer Overflow	web.archive.org text/html	SECUNIA 16764
MFSA 2005-57: IDN heap overrun using soft-hyphens	www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/mfsa2005-57.html
Debian -- Security Information -- DSA-866-1 mozilla	www.debian.org Depreciated Link text/html	DEBIAN DSA-866
Secunia - Advisories - Fedora update for thunderbird	web.archive.org text/html	SECUNIA 17042
SecurityReason - HP-UX Mozilla Remote Unauthorized Execution of Privileged Code or Denial of Service (DoS)	securityreason.com text/html	SREASON 83
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mozilla-url-bo(22207)
No Description Provided	Exploit Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.security-protocols.com/advisory/sp-x17-advisory.txt
307259 – Firefox 1.0.6 buffer overflow with hostname of all soft hyphens [@ nsStringBuffer::Realloc] [@ nsCSubstring::Capacity] [@ nsGenericElement::~nsGenericElement]	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=307259
Debian -- Security Information -- DSA-837-1 mozilla-firefox	www.debian.org Depreciated Link text/html	DEBIAN DSA-837
US-CERT Vulnerability Note VU#573857	US Government Resource www.kb.cert.org text/html	CERT-VN VU#573857
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:9608
Secunia - Advisories - Debian update for mozilla	web.archive.org text/html	SECUNIA 17263
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:769
Support	www.redhat.com text/html	REDHAT RHSA-2005:768
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-1690
Secunia - Advisories - Red Hat update for thunderbird	web.archive.org text/html	SECUNIA 17090

Secunia - Advisories - Mozilla IDN URL Domain Name Buffer Overflow	web.archive.org text/html	SECUNIA 16767
SecuriTeam.com ™ - Gecko Based Browser IDN Buffer Overflow	www.securiteam.com text/html	MISC www.securiteam.com/securitynews/5RP0B0UGVW.html
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:791
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-1824
usn/usn-181-1 - Ubuntu Linux	www.ubuntu.com text/html	UBUNTU USN-181-1
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1287
Secunia - Advisories - Netscape IDN URL Domain Name Buffer Overflow	web.archive.org text/html	SECUNIA 16766
SecurityTracker.com Archives - Mozilla Firefox Buffer Overflow in Processing Hostnames May Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1014877
No Description Provided	Exploit web.archive.org text/html Inactive Link Not Archived	MISC www.security-protocols.com/firefox-death.html
Neohapsis Archives - Full Disclosure List - #0316 - [Full-disclosure] FireFox "Host:" Buffer Overflow is not just exploitable on FireFox	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20050911 FireFox "Host:" Buffer Overflow is not just exploitable on FireFox
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-1691
Mozilla/Netscape/Firefox Browsers Domain Name Remote Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 14784
'[Full-disclosure] Mozilla Firefox "Host:" Buffer Overflow' - MARC	marc.info text/html	FULLDISC 20050909 Mozilla Firefox "Host:" Buffer Overflow
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:584

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	1.0.6	All	All	All
Application	Mozilla	Firefox	1.5	beta1	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	1.0.6	All	All	All
Application	Mozilla	Firefox	1.5	beta1	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:1.0.6:*:*:*:*:*:*:*:
- cpe:2.3:a:mozilla:firefox:1.5:beta1:*:*:*:*:*:*:
- 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:1.0.6:*:*:*:*:*:*:*:
- cpe:2.3:a:mozilla:firefox:1.5:beta1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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