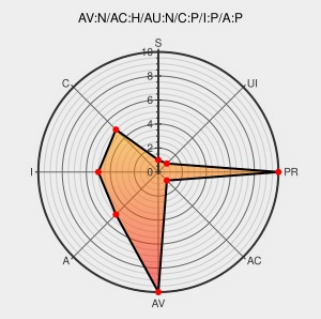
CVE-2006-1993

Published on: 04/25/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1993

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



Certain versions of Firefox from Mozilla contain the following vulnerability:

Mozilla Firefox 1.5.0.2, when designMode is enabled, allows remote attackers to cause a denial of service and possibly execute arbitrary code via certain Javascript that is not properly handled by the contentWindow.focus method in an iframe, which causes a reference to a deleted controller context object. NOTE: this was originally claimed to be a buffer overflow in (1) js320.dll and (2) xpcom_core.dll, but the vendor disputes this claim.

CVE-2006-1993 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5.1 - MEDIUM

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-1053-1 mozilla	www.debian.org Depreciated Link text/html	DEBIAN DSA-1053
Webmail- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-1922
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060424 Firefox Remote Code Execution and DoS 1.5.0.2
SecurityReason - Firefox Remote Code Execution and DoS 1.5.0.2	securityreason.com text/html	SREASON 780

SecurityFocus	www.securityfocus.com text/html	HP SSRT061181
Debian -- Security Information -- DSA-1055-1 mozilla-firefox	www.debian.org Depreciated Link text/html	DEBIAN DSA-1055
HP-UX update for firefox - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22066
Firefox "contentWindow.focus()" Deleted Object Reference Vulnerability - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 19802
Gentoo update for mozilla-firefox - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 20019
Gentoo Linux Documentation -- Mozilla Firefox: Potential remote code execution	www.gentoo.org text/html	GENTOO GLSA-200605-06
MFSA 2006-30: Deleted object reference when designMode="on"	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2006/mfsa2006-30.html
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1790
Webmail- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-1614
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2008-0083
US-CERT Vulnerability Note VU#866300	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#866300
Secunia - Advisories - Debian update for mozilla-firefox	Vendor Advisory web.archive.org text/html	SECUNIA 20070
Debian update for mozilla - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 20015
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-3748
HP Tru64 UNIX Firefox/Mozilla Application Suite Vulnerability - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 20214
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF firefox-iframe-contentwindowfocus-bo(25994)
SecurityFocus	www.securityfocus.com text/html	HP SSRT061145
No Description Provided	Exploit www.securident.com text/html	MISC www.securident.com/vuln/ff.txt

SecurityTracker.com Archives - Firefox IFRAME Initialization Function Lets Remote Users Execute Arbitrary Code	Exploit securitytracker.com text/html	SECTRACK 1015981
Mozilla Firefox iframe.contentWindow.focus Deleted Object Reference Vulnerability	Exploit Patch cve.report (archive) text/html	BID 17671

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	1.5.0.2	All	All	All
Application	Mozilla	Firefox	1.5.0.2	All	All	All

cpe:2.3:a:mozilla:firefox:1.5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:1.5.0.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→