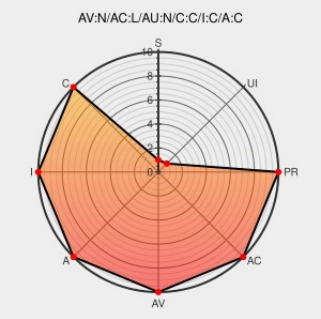
CVE-2010-1121

Published on: 03/25/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:05 PM UTC

CVE-2010-1121

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



Certain versions of Firefox from Mozilla contain the following vulnerability:

Mozilla Firefox 3.6.x before 3.6.3 does not properly manage the scopes of DOM nodes that are moved from one document to another, which allows remote attackers to conduct use-after-free attacks and execute arbitrary code via unspecified vectors involving improper interaction with garbage collection, as demonstrated by Nils during a Pwn2Own competition at CanSecWest 2010.

CVE-2010-1121 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
[security-announce] SUSE Security Announcement: Mozilla Firefox (SUSE-SA	lists.opensuse.org text/html	SUSE SUSE-SA:2010:030
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10924
555109 – (CVE-2010-1121) Move wrappers to new scope even if their parent hasn't been moved yet (ZDI-CAN-761)	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=555109
[SECURITY] Fedora 13 Update: firefox-3.6.4-1.fc13	lists.fedoraproject.org text/html	FEDORA FEDORA-2010-10361
Webmail : Solution de messagerie professionnelle -	www.vupen.com	VUPEN ADV-2010-1592

OVHcloud- OVH	text/html	
MFSA 2010-25: Re-use of freed object due to scope confusion	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2010/mfsa2010-25.html
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2010-1557
[SECURITY] Fedora 12 Update: firefox-3.5.10-1.fc12	lists.fedoraproject.org text/html	FEDORA FEDORA-2010-10344
SecurityTracker.com Archives - Mozilla Firefox Memory Re-use Error Lets Remote Users Execute Arbitrary Code	www.securitytracker.com text/html	SECTRACK 1023817
Mozilla Thunderbird Multiple Vulnerabilities - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 40323
Mozilla SeaMonkey Multiple Vulnerabilities - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 40326
ASA-2010-165 (RHSA-2010-0500)	support.avaya.com text/html	CONFIRM support.avaya.com/css/P8/documents/100091069
Support | Red Hat	www.redhat.com text/html	REDHAT RHSA-2010:0501
Threat Intelligence | Digital Vaccine® | ThreatLinQ | Trend Micro	dvlabs.tippingpoint.com text/html	MISC dvlabs.tippingpoint.com/blog/2010/02/15/pwn2own-2010
Zero Day Initiative on Twitter: "Nils from MWR InfoSecurity (@MWRLabs) succeeded against Firefox on Windows 7 with the quintessential calc.exe launching payload."	nitter.domain.glass text/html	MISC twitter.com/thezdi/statuses/11005277222
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2010-1640
Support	www.redhat.com text/html	REDHAT RHSA-2010:0500
iPhone, Safari, IE 8, Firefox hacked in CanSecWest contest | InSecurity Complex - CNET News	web.archive.org text/html Inactive Link Not Archived	MISC news.cnet.com/8301-27080_3-20001126-245.html
SUSE update for MozillaFirefox and mozilla-xulrunner191 - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 40481
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2010-1773
Ubuntu update for firefox and xulrunner - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 40401
USN-930-1: Firefox and Xulrunner vulnerabilities | Ubuntu	ubuntu.com text/html	UBUNTU USN-930-1
USN-930-2: apturl, Epiphany, gecko-sharp, gnome-python-extras, liferea, rhythmbox, totem, ubufox, yelp update | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-930-2

Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:6844

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	3.6	All	All	All
Application	Mozilla	Firefox	3.6.1	All	All	All
Application	Mozilla	Firefox	3.6.2	All	All	All
Application	Mozilla	Firefox	3.6	All	All	All
Application	Mozilla	Firefox	3.6.1	All	All	All
Application	Mozilla	Firefox	3.6.2	All	All	All

cpe:2.3:a:mozilla:firefox:3.6:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:3.6.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→