



CVE-2006-3677

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2006-3677
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-07-27 19:04:00 UTC
Updated	2018-10-18 16:48:00 UTC
Description	Mozilla Firefox 1.5 before 1.5.0.5 and SeaMonkey before 1.0.3 allows remote attackers to execute arbitrary code by changi

Risk And Classification

Problem Types: CWE-16

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	1.5	All	All	All
Application	Mozilla	Firefox	1.5.0.1	All	All	All
Application	Mozilla	Firefox	1.5.0.2	All	All	All
Application	Mozilla	Firefox	1.5.0.3	All	All	All
Application	Mozilla	Firefox	1.5.0.4	All	All	All
Application	Mozilla	Firefox	1.5	All	All	All
Application	Mozilla	Firefox	1.5.0.1	All	All	All
Application	Mozilla	Firefox	1.5.0.2	All	All	All
Application	Mozilla	Firefox	1.5.0.3	All	All	All
Application	Mozilla	Firefox	1.5.0.4	All	All	All
Application	Mozilla	Seamonkey	1.0	All	All	All
Application	Mozilla	Seamonkey	1.0	All	dev	All
Application	Mozilla	Seamonkey	1.0.1	All	All	All
Application	Mozilla	Seamonkey	1.0.2	All	All	All
Application	Mozilla	Seamonkey	1.0	All	All	All
Application	Mozilla	Seamonkey	1.0	All	dev	All
Application	Mozilla	Seamonkey	1.0.1	All	All	All

Application	Mozilla	Seamonkey	1.0.2	All	All	All
References						
Reference				Source	Link	
ZDI-06-025 Zero Day Initiative				MISC	www.zeroday.in	
rhn.redhat.com Red Hat Support				REDHAT	rhn.redhat.com	
Mozilla Firefox Multiple Vulnerabilities - Advisories - Secunia				SECUNIA	secunia.com	
SecurityFocus				HP	www.securityfocus.com	
[#RPL-536] update firefox to 1.5.0.5 for security issues - rPath JIRA				CONFIRM	issues.rpath.com	
US-CERT Vulnerability Note VU#670060				CERT-VN	www.kb.cert.org	
IBM X-Force Exchange				XF	exchange.xforce	
HP-UX update for firefox - Advisories - Secunia				SECUNIA	secunia.com	
SecurityTracker.com Archives - Mozilla Seamonkey Multiple Bugs Let Remote Users Execute Arbitrary Code				SECTRAK	securitytracker.com	
Gentoo update for seamonkey - Advisories - Secunia				SECUNIA	secunia.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen.com	
SecurityFocus				BUGTRAQ	www.securityfocus.com	
Mozilla SeaMonkey Multiple Vulnerabilities - Advisories - Secunia				SECUNIA	secunia.com	
Mozilla Multiple Products Remote Vulnerabilities				BID	www.securityfocus.com	
US-CERT Technical Cyber Security Alert TA06-208A -- Mozilla Products Contain Multiple Vulnerabilities				CERT	www.us-cert.gov	
rhn.redhat.com Red Hat Support				REDHAT	www.redhat.com	
Advisories - Mandriva Linux				MANDRIVA	www.mandriva.com	
SUSE update for MozillaFirefox, MozillaThunderbird, and Seamonkey - Advisories - Secunia				SECUNIA	secunia.com	
usn/usn-354-1 - Ubuntu: Linux for human beings				UBUNTU	www.ubuntu.com	
Red Hat update for seamonkey - Advisories - Secunia				SECUNIA	secunia.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen.com	
SecurityFocus				BUGTRAQ	www.securityfocus.com	
Repository / Oval Repository				OVAL	oval.cisecurity.com	
Ubuntu update for firefox - Advisories - Secunia				SECUNIA	secunia.com	
Ubuntu update for firefox - Advisories - Secunia				SECUNIA	secunia.com	
rPath update for firefox - Advisories - Secunia				SECUNIA	secunia.com	
Mandriva update for mozilla-firefox - Advisories - Secunia				SECUNIA	secunia.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen.com	
IBM X-Force Exchange				XF	exchange.xforce	
Gentoo update for mozilla-firefox - Advisories - Secunia				SECUNIA	secunia.com	
MFSA 2006-45: Javascript navigator Object Vulnerability				CONFIRM	www.mozilla.org	

rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com
Red Hat update for seamonkey - Advisories - Secunia	SECUNIA	secunia.com
Mozilla Firefox Javascript Navigator Object Remote Code Execution Vulnerability	BID	www.securityfocus.com
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia	SECUNIA	secunia.com
Gentoo Linux Documentation -- Mozilla SeaMonkey: Multiple vulnerabilities	GENTOO	security.gentoo.org
20060703-01-P	SGI	patches.sgi.com
Security Announcement	SUSE	www.novell.com
Advisories - Mandriva Linux	MANDRIVA	www.mandriva.com
SecurityTracker.com Archives - Mozilla Firefox Multiple Bugs Let Remote Users Execute Arbitrary Code	SECTrack	securitytracker.com
Red Hat update for seamonkey - Advisories - Secunia	SECUNIA	secunia.com
USN-327-1: firefox vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com
Gentoo Linux Documentation -- Mozilla Firefox: Multiple vulnerabilities	GENTOO	www.gentoo.org
Red Hat update for thunderbird - Advisories - Secunia	SECUNIA	secunia.com
Red Hat update for firefox - Advisories - Secunia	SECUNIA	secunia.com
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.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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