



CVE-2006-6504

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

Summary

CVE	CVE-2006-6504
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-20 01:28:00 UTC
Updated	2018-10-17 21:48:00 UTC
Description	Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to execute arbitrary code via crafted SVG files.

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	5.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	5.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All

References

Reference
Gentoo update for seamonkey - Advisories - Secunia
US-CERT Vulnerability Note VU#928956
Mozilla Seamonkey SVG Processing Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker
Red Hat update for thunderbird - Advisories - Secunia

Gentoo Linux Documentation -- SeaMonkey: Multiple vulnerabilities
Red Hat update for seamonkey - Advisories - Secunia
SecurityFocus
Mozilla Firefox/SeaMonkey/Thunderbird Multiple Remote Vulnerabilities
Ubuntu update for firefox - Advisories - Secunia
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia
20061202-01-P
MFSA 2006-73: Mozilla SVG Processing Remote Code Execution
SecurityFocus
Fedora update for thunderbird - Advisories - Secunia
rPath update for thunderbird - Advisories - Secunia
SecurityFocus
rhn.redhat.com Red Hat Support
Security Announcement
SUSE updates for MozillaFirefox and MozillaThunderbird - Advisories - Secunia
Mozilla Firefox Multiple Vulnerabilities - Advisories - Secunia
rPath update for firefox - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
rhn.redhat.com Red Hat Support
usn/usn-398-2 - Ubuntu: Linux for human beings
HPSBUX02153 SSRT061181 rev.7 - HP-UX Running Firefox, Remote Unauthorized Access or Elevation of Privileges or Denial of Service (DoS)
US-CERT Technical Cyber Security Alert TA06-354A -- Mozilla Addresses Multiple Vulnerabilities
SUSE update for mozilla - Advisories - Secunia
ZDI-06-051
Repository / Oval Repository
issues.rpath.com/browse/RPL-883
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
rhn.redhat.com Red Hat Support
Advisories - Mandriva Linux
usn/USN-398-1 - Ubuntu: Linux for human beings
Gentoo Linux Documentation -- Mozilla Firefox: Multiple vulnerabilities
[SECURITY] Fedora Core 5 Update: thunderbird-1.5.0.9-2.fc5 FedoraNEWS.ORG
Mozilla Firefox SVG Processing Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker
Security Announcement
[SECURITY] Fedora Core 6 Update: thunderbird-1.5.0.9-2.fc6 FedoraNEWS.ORG
Download Firefox 1.5.0.9-2.fc6 RPMs

Hed Hat update for firefox - Advisories - Secunia
Gentoo update for mozilla-firefox - Advisories - Secunia
Mozilla SeaMonkey Multiple Vulnerabilities - Advisories - Secunia
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)