



CVE-2006-6500

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

Summary

CVE	CVE-2006-6500
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-20 01:28:00 UTC
Updated	2019-10-09 22:51:00 UTC
Description	Heap-based buffer overflow in Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.1.18.0.1

Risk And Classification

Problem Types: CWE-119

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
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	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
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

References
Reference
Gentoo update for seamonkey - Advisories - Secunia
Gentoo Linux Documentation -- SeaMonkey: Multiple vulnerabilities
Mozilla Thunderbird Multiple Vulnerabilities - Advisories - Secunia
Mozilla Seamonkey Windows Cursor Image Conversion Heap Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker
Mozilla Firefox/SeaMonkey/Thunderbird Multiple Remote Vulnerabilities
Mozilla Thunderbird Windows Cursor Image Conversion Heap Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker
Security Announcement
SUSE updates for MozillaFirefox and MozillaThunderbird - Advisories - Secunia
Mozilla Firefox Multiple Vulnerabilities - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Gentoo Linux Documentation -- Mozilla Thunderbird: Multiple vulnerabilities
US-CERT Technical Cyber Security Alert TA06-354A -- Mozilla Addresses Multiple Vulnerabilities
SUSE update for mozilla - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Advisories - Mandriva Linux
Advisories - Mandriva Linux
HPSBUX02153 SSRT061181 rev.7 - HP-UX Running Firefox, Remote Unauthorized Access or Elevation of Privileges or Denial of Service (DoS)
Gentoo Linux Documentation -- Mozilla Firefox: Multiple vulnerabilities
Security Announcement
Mozilla Firefox Windows Cursor Image Conversion Heap Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker
US-CERT Vulnerability Note VU#722244
Gentoo update for mozilla-firefox - Advisories - Secunia
Gentoo update for mozilla-thunderbird - Advisories - Secunia
Mozilla SeaMonkey Multiple Vulnerabilities - Advisories - Secunia
MFSA 2006-69: CSS cursor image buffer overflow (Windows only)
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.

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