



CVE-2006-1723

Published on: 04/14/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

CVE-2006-1723

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Firefox](#) from [Mozilla](#) contain the following vulnerability:

Unspecified vulnerability in Firefox and Thunderbird before 1.5.0.2, and SeaMonkey before 1.0.1, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown attack vectors related to DHTML. NOTE: due to the lack of sufficient public details from the vendor as of 20060413, it is unclear how CVE-2006-1529, CVE-2006-1530, CVE-2006-1531, and CVE-2006-1723 are different.

CVE-2006-1723 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityTracker.com Archives - Mozilla Seamonkey Memory Corruption in Processing DHTML May Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTrack 1015919
Mozilla SeaMonkey Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 19649
Debian -- Security Information -- DSA-1051-1 mozilla-thunderbird	www.debian.org Deprecated Link text/html	DEBIAN DSA-1051
SecurityFocus	www.securityfocus.com text/html	HP SSRT061181

Mozilla Suite, Firefox, SeaMonkey, and Thunderbird Multiple Remote Vulnerabilities	cve.report (archive) text/html	 BID 17516
HP-UX update for firefox - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22066
SecurityFocus	www.securityfocus.com text/html	 HP SSRT061236
Debian -- Security Information -- DSA-1046-1 mozilla	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1046
Mozilla Thunderbird Memory Corruption in Processing DHTML May Let Remote Users Execute Arbitrary Code - SecurityTracker	securitytracker.com text/html	 SECTrack 1015920
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2008-0083
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1574
Firefox Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 19631
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2006-3748
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2006-1356
Debian update for mozilla - Advisories - Secunia	web.archive.org text/html	 SECUNIA 19863
HP-UX update for thunderbird - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22065
SecurityTracker.com Archives - Mozilla Firefox Memory Corruption in Processing DHTML May Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	 SECTrack 1015921
Debian update for mozilla-thunderbird - Advisories - Secunia	web.archive.org text/html	 SECUNIA 19941
UnixWare update for mozilla - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21033
MFSA 2006-20: Crashes with evidence of memory corruption (rv:1.8.0.2)	www.mozilla.org text/html	 CONFIRM www.mozilla.org/security/announce/2006/mfsa2006-20.html
	ftp.sco.com text/plain	 SCO SCOSA-2006.26
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2006-3749
US-CERT Vulnerability Note VU#350262	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#350262

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	1.0	All	All	All
Application	Mozilla	Firefox	1.0.1	All	All	All
Application	Mozilla	Firefox	1.0.2	All	All	All
Application	Mozilla	Firefox	1.0.3	All	All	All
Application	Mozilla	Firefox	1.0.4	All	All	All
Application	Mozilla	Firefox	1.0.5	All	All	All
Application	Mozilla	Firefox	1.0.6	All	All	All
Application	Mozilla	Firefox	1.0.7	All	All	All
Application	Mozilla	Firefox	1.5	All	All	All
Application	Mozilla	Firefox	1.5	beta1	All	All
Application	Mozilla	Firefox	1.5	beta2	All	All
Application	Mozilla	Firefox	1.5.0.1	All	All	All
Application	Mozilla	Firefox	preview_release	All	All	All
Application	Mozilla	Firefox	1.0	All	All	All
Application	Mozilla	Firefox	1.0.1	All	All	All
Application	Mozilla	Firefox	1.0.2	All	All	All
Application	Mozilla	Firefox	1.0.3	All	All	All
Application	Mozilla	Firefox	1.0.4	All	All	All
Application	Mozilla	Firefox	1.0.5	All	All	All
Application	Mozilla	Firefox	1.0.6	All	All	All
Application	Mozilla	Firefox	1.0.7	All	All	All
Application	Mozilla	Firefox	1.5	All	All	All
Application	Mozilla	Firefox	1.5	beta1	All	All
Application	Mozilla	Firefox	1.5	beta2	All	All
Application	Mozilla	Firefox	1.5.0.1	All	All	All
Application	Mozilla	Firefox	preview_release	All	All	All
Application	Mozilla	Seamonkey	1.0	All	alpha	All
Application	Mozilla	Seamonkey	1.0	beta	All	All
Application	Mozilla	Seamonkey	1.0	All	alpha	All
Application	Mozilla	Seamonkey	1.0	beta	All	All
Application	Mozilla	Thunderbird	1.0	All	All	All

Application	Mozilla	Thunderbird	1.0.1	All	All	All
Application	Mozilla	Thunderbird	1.0.2	All	All	All
Application	Mozilla	Thunderbird	1.0.3	All	All	All
Application	Mozilla	Thunderbird	1.0.4	All	All	All
Application	Mozilla	Thunderbird	1.0.5	All	All	All
Application	Mozilla	Thunderbird	1.0.5	beta	All	All
Application	Mozilla	Thunderbird	1.0.6	All	All	All
Application	Mozilla	Thunderbird	1.0.7	All	All	All
Application	Mozilla	Thunderbird	1.5	All	All	All
Application	Mozilla	Thunderbird	1.5	beta2	All	All
Application	Mozilla	Thunderbird	1.5.0.1	All	All	All
Application	Mozilla	Thunderbird	1.0	All	All	All
Application	Mozilla	Thunderbird	1.0.1	All	All	All
Application	Mozilla	Thunderbird	1.0.2	All	All	All
Application	Mozilla	Thunderbird	1.0.3	All	All	All
Application	Mozilla	Thunderbird	1.0.4	All	All	All
Application	Mozilla	Thunderbird	1.0.5	All	All	All
Application	Mozilla	Thunderbird	1.0.5	beta	All	All
Application	Mozilla	Thunderbird	1.0.6	All	All	All
Application	Mozilla	Thunderbird	1.0.7	All	All	All
Application	Mozilla	Thunderbird	1.5	All	All	All
Application	Mozilla	Thunderbird	1.5	beta2	All	All
Application	Mozilla	Thunderbird	1.5.0.1	All	All	All
cpe:2.3:a:mozilla:firefox:1.0:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.0.1:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.0.2:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.0.3:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.0.4:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.0.5:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.0.6:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.0.7:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5:beta1:*:*:*:*:*:						

cpe:2.3:a:mozilla:firefox:1.5:beta2:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.5.0.1:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:preview_release:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.0:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.0.1:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.0.2:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.0.3:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.0.4:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.0.5:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.0.6:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.0.7:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.5:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.5:beta1:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.5:beta2:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:1.5.0.1:*:*:*:*:*:
cpe:2.3:a:mozilla:firefox:preview_release:*:*:*:*:*:
cpe:2.3:a:mozilla:seamonkey:1.0:*:alpha:*:*:*:*:
cpe:2.3:a:mozilla:seamonkey:1.0:beta:*:*:*:*:
cpe:2.3:a:mozilla:seamonkey:1.0:*:alpha:*:*:*:*:
cpe:2.3:a:mozilla:seamonkey:1.0:beta:*:*:*:*:
cpe:2.3:a:mozilla:thunderbird:1.0:*:*:*:*:*:
cpe:2.3:a:mozilla:thunderbird:1.0.1:*:*:*:*:*:
cpe:2.3:a:mozilla:thunderbird:1.0.2:*:*:*:*:*:
cpe:2.3:a:mozilla:thunderbird:1.0.3:*:*:*:*:*:
cpe:2.3:a:mozilla:thunderbird:1.0.4:*:*:*:*:*:
cpe:2.3:a:mozilla:thunderbird:1.0.5:*:*:*:*:*:
cpe:2.3:a:mozilla:thunderbird:1.0.5:beta:*:*:*:*:
cpe:2.3:a:mozilla:thunderbird:1.0.6:*:*:*:*:*:

cpe:2.3:a:mozilla:thunderbird:1.0.7:*****:
cpe:2.3:a:mozilla:thunderbird:1.5:*****:
cpe:2.3:a:mozilla:thunderbird:1.5:beta2:*****:
cpe:2.3:a:mozilla:thunderbird:1.5.0.1:*****:
cpe:2.3:a:mozilla:thunderbird:1.0:*****:
cpe:2.3:a:mozilla:thunderbird:1.0.1:*****:
cpe:2.3:a:mozilla:thunderbird:1.0.2:*****:
cpe:2.3:a:mozilla:thunderbird:1.0.3:*****:
cpe:2.3:a:mozilla:thunderbird:1.0.4:*****:
cpe:2.3:a:mozilla:thunderbird:1.0.5:*****:
cpe:2.3:a:mozilla:thunderbird:1.0.5:beta:*****:
cpe:2.3:a:mozilla:thunderbird:1.0.6:*****:
cpe:2.3:a:mozilla:thunderbird:1.0.7:*****:
cpe:2.3:a:mozilla:thunderbird:1.5:*****:
cpe:2.3:a:mozilla:thunderbird:1.5:beta2:*****:
cpe:2.3:a:mozilla:thunderbird:1.5.0.1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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](#).

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