



# CVE-2006-2784

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

## Summary

<b>CVE</b>	CVE-2006-2784
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-06-02 19:02:00 UTC
<b>Updated</b>	2018-10-18 16:42:00 UTC
<b>Description</b>	The PLUGINSFAGE functionality in Mozilla Firefox before 1.5.0.4 allows remote user-assisted attackers to execute privileg

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All

## References

### Reference

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Gentoo Linux Documentation -- Mozilla Firefox: Multiple vulnerabilities
rhn.redhat.com   Red Hat Support
Ubuntu update for mozilla-thunderbird - Advisories - Secunia
SecurityFocus
Security Announcement
Debian update for mozilla-thunderbird - Advisories - Secunia
USN-296-1: firefox vulnerabilities   Ubuntu security notices
HP-UX update for firefox - Advisories - Secunia
Firefox Multiple Vulnerabilities - Advisories - Secunia
Debian -- Security Information -- DSA-1134-1 mozilla-thunderbird
SecurityTracker.com Archives - Mozilla Firefox Bugs Permit Arbitrary Code Execution, Cross-Site Scripting, and HTTP Response Smuggling
USN-297-3: Thunderbird vulnerabilities   Ubuntu security notices

[rh.n.redhat.com | Red Hat Support](#)

[MFSA 2006-36: PLUGINSPAGE privileged JavaScript execution 2](#)

[Advisories - Mandriva Linux](#)

[Debian -- Security Information -- DSA-1118-1 mozilla](#)

[Red Hat update for seamonkey - Advisories - Secunia](#)

[SecurityFocus](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[Repository / Oval Repository](#)

[rh.n.redhat.com | Red Hat Support](#)

[Debian update for mozilla - Advisories - Secunia](#)

[Mandriva update for mozilla-firefox - Advisories - Secunia](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[Debian -- Security Information -- DSA-1120-1 mozilla-firefox](#)

[USN-323-1: mozilla vulnerabilities | Ubuntu security notices](#)

[rh.n.redhat.com | Red Hat Support](#)

[rh.n.redhat.com | Red Hat Support](#)

[Debian update for mozilla-firefox - Advisories - Secunia](#)

[Mozilla Firefox, SeaMonkey, Camino, and Thunderbird Multiple Remote Vulnerabilities](#)

[Advisories - Mandriva Linux](#)

[Ubuntu update for firefox - Advisories - Secunia](#)

[Red Hat update for seamonkey - Advisories - Secunia](#)

[USN-296-2: Firefox vulnerabilities | Ubuntu security notices](#)

[IBM X-Force Exchange](#)

[Red Hat update for thunderbird - Advisories - Secunia](#)

[Gentoo update for firefox - Advisories - Secunia](#)

[Red Hat update for firefox - Advisories - Secunia](#)

[Ubuntu update for mozilla - Advisories - Secunia](#)

[Red Hat update for seamonkey - 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](#)