



CVE-2006-2778

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2006-2778
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-02 18:02:00 UTC
Updated	2018-10-18 16:42:00 UTC
Description	The crypto.signText function in Mozilla Firefox and Thunderbird before 1.5.0.4 allows remote attackers to execute arbitrary

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

US-CERT Technical Cyber Security Alert TA06-153A -- Mozilla Products Contain Multiple Vulnerabilities

#102763: Multiple Security Vulnerabilites in Mozilla 1.7 for Solaris 8, 9, and 10

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

MFSA 2006-38: Buffer overflow in crypto.signText()

SecurityFocus

Security Announcement

Debian update for mozilla-thunderbird - Advisories - Secunia

IBM X-Force Exchange

USN-296-1: firefox vulnerabilities | Ubuntu security notices

HP-UX update for firefox - Advisories - Secunia
SecurityFocus
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
rhn.redhat.com Red Hat Support
Gentoo Linux Documentation -- Mozilla Thunderbird: Multiple vulnerabilities
Advisories - Mandriva Linux
Debian -- Security Information -- DSA-1118-1 mozilla
Red Hat update for seamonkey - Advisories - Secunia
Thunderbird Multiple Vulnerabilities - Advisories - Secunia
SecurityFocus
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
rhn.redhat.com Red Hat Support
USN-297-1: Thunderbird vulnerabilities Ubuntu security notices
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
SecurityTracker.com Archives - Mozilla Thunderbird Bugs Permit Arbitrary Code Execution, Cross-Site Scripting, and HTTP Response Smugg
rhn.redhat.com Red Hat Support
rhn.redhat.com Red Hat Support
Mandriva update for mozilla-thunderbird - Advisories - Secunia
Debian update for mozilla-firefox - Advisories - Secunia
Mozilla Firefox, SeaMonkey, Camino, and Thunderbird Multiple Remote Vulnerabilities
HP-UX update for thunderbird - Advisories - Secunia
Gentoo update for mozilla-thunderbird - Advisories - Secunia
US-CERT Vulnerability Note VU#421529
Advisories - Mandriva Linux
Advisories - Mandriva Linux
Ubuntu update for firefox - Advisories - Secunia
Repository / Oval Repository
Red Hat update for seamonkey - Advisories - Secunia
USN-323-1: mozilla vulnerabilities Ubuntu security notices

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Red Hat update for thunderbird - Advisories - Secunia

Gentoo update for firefox - Advisories - Secunia

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

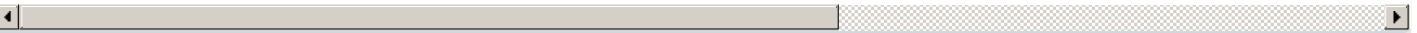
Red Hat update for firefox - Advisories - Secunia

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](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://cve.mitre.org). 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