CVE-2006-0884

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2006-0884
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-24 22:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The WYSIWYG rendering engine ("rich mail" editor) in Mozilla Thunderbird 1.0.7 and earlier allows user-assisted attackers

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

EPSS: 0.359970000 probability, percentile 0.970960000 (date 2026-04-16)

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Mozilla	Thunderbird	0.1	All	All	All
Application	Mozilla	Thunderbird	0.2	All	All	All
Application	Mozilla	Thunderbird	0.3	All	All	All
Application	Mozilla	Thunderbird	0.4	All	All	All
Application	Mozilla	Thunderbird	0.5	All	All	All
Application	Mozilla	Thunderbird	0.6	All	All	All
Application	Mozilla	Thunderbird	0.7	All	All	All
Application	Mozilla	Thunderbird	0.7.1	All	All	All
Application	Mozilla	Thunderbird	0.7.2	All	All	All
Application	Mozilla	Thunderbird	0.7.3	All	All	All
Application	Mozilla	Thunderbird	0.8	All	All	All
Application	Mozilla	Thunderbird	0.9	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	1.0.5	All	All	All
Application	Mozilla	Thunderbird	1.0.6	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
SUSE update for mozilla/firefox - Advisories - Secunia
Debian update for mozilla-thunderbird - Advisories - Secunia
Sun Solaris update for mozilla - Advisories - Secunia
Debian -- Security Information -- DSA-1051-1 mozilla-thunderbird
USN-276-1: Thunderbird vulnerabilities | Ubuntu security notices
Gentoo Linux Documentation -- Mozilla Suite: Multiple vulnerabilities
MFSA 2006-21: JavaScript execution in mail when forwarding in-line
ASA-2006-205 (SUN 102502, 102513, 102514, 102519, 102550, 102556, 102557, 102582, 102588, 102589, 102593)
sunsolve.sun.com/search/document.do
Repository / Oval Repository
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SUSE update for MozillaThunderbird - Advisories - Secunia
Advisories - Mandriva Linux
SGI Advanced Linux Environment 3 Multiple Updates - Advisories - Secunia
Gentoo update for mozilla - Advisories - Secunia
Secunia - Advisories - Gentoo update for mozilla-thunderbird
SecurityFocus
SecurityFocus
Security Announcement
Debian update for mozilla - Advisories - Secunia
patches.sgi.com/support/free/security/advisories/20060404-01-U.asc
Ubuntu update for thunderbird - Advisories - Secunia
HP-UX update for thunderbird - Advisories - Secunia
ftp.sco.com/pub/updates/UnixWare/SCOSA-2006.26/SCOSA-2006.26.txt
SecurityFocus
Advisories - Mandriva Linux
SecurityFocus
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: Mozilla Firefox, Mozilla Suite various problems (SU
SecurityTracker.com Archives - Mozilla Thunderbird Validation Error in IFRAME SRC Tag Lets Remote Users Execute Arbitrary Javascript
rhn.redhat.com | Red Hat Support
Mandriva update for mozilla-thunderbird - Advisories - Secunia
Gentoo Linux Documentation -- Mozilla Thunderbird: Multiple vulnerabilities
Debian -- Security Information -- DSA-1046-1 mozilla
Repository / Oval Repository
rhn.redhat.com | Red Hat Support
Advisories - Mandriva Linux
IBM X-Force Exchange
www.osvdb.org/23653
Multiple Mozilla Products IFRAME JavaScript Execution Vulnerability
UnixWare update for mozilla - Advisories - Secunia
#102550: Multiple Security Vulnerabilites in Mozilla 1.4 and 1.7 for Solaris and for Sun JDS for Linux
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy OID mappings associated with this CVE

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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