CVE-2007-3736

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

Summary

CVE	CVE-2007-3736
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-07-18 17:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 2.0.0.5 allows remote attackers to inject arbitrary web script

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	2.0	All	All	All

Application	Mozilla	Firefox	2.0.0.1	All	All	All
Application	Mozilla	Firefox	2.0.0.2	All	All	All
Application	Mozilla	Firefox	2.0.0.3	All	All	All
Application	Mozilla	Firefox	2.0.0.4	All	All	All

Vendor Declared Affected Products

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

References

Reference
Red Hat update for seamonkey - Advisories - Secunia
Gentoo Linux Documentation -- Mozilla products: Multiple vulnerabilities
Advisories | Mandriva
SecurityFocus
#201516: Multiple Security Vulnerabilities in Firefox and Thunderbird for Solaris 10 May Allow Execution of Arbitrary Code and Access to Unau
Debian update for xulrunner - Advisories - Secunia
Debian update for iceweasel - Advisories - Secunia
Slackware update for thunderbird - Advisories - Secunia
Mozilla Firefox 2.0.0.4 Multiple Remote Vulnerabilities
Red Hat update for firefox - Advisories - Secunia
Security update for MozillaFirefox
#201516: Multiple Security Vulnerabilities in Firefox and Thunderbird for Solaris 10 May Allow Execution of Arbitrary Code and Access to Unau
SUSE update for MozillaFirefox - Advisories - Secunia
MFSA 2007-19: XSS using addEventListener and setTimeout
rhn.redhat.com | Red Hat Support
Security Announcement
SUSE update for MozillaFirefox, MozillaThunderbird, and Seamonkey - Advisories - Secunia
Debian -- Security Information -- DSA-1337-1 xulrunner
Debian update for iceape - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
rPath update for firefox and thunderbird - Advisories - Secunia
rhn.redhat.com | Red Hat Support
ftp.slackware.com/pub/slackware/slackware-12.0/ChangeLog.txt
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia
HPSBUX02153 SSRT061181 rev.7 - HP-UX Running Firefox, Remote Unauthorized Access or Elevation of Privileges or Denial of Service (Do
Debian -- Security Information -- DSA-1339-1 iceape

Debian -- Security Information -- DSA-1339-1 iceape
patches.sgi.com/support/free/security/advisories/20070701-01-P.asc
Mandriva update for mozilla-firefox - Advisories - Secunia
Red Hat update for thunderbird - Advisories - Secunia
Webmail - OVH
Gentoo update for Mozilla Products - Advisories - Secunia
Slackware update for firefox - Advisories - Secunia
Slackware update for seamonkey - Advisories - Secunia
Sun Solaris Firefox / Thunderbird Multiple Vulnerabilities - Advisories - Secunia
Repository / Oval Repository
Mozilla Firefox addEventListener() or setTimeout() Functions Permit Cross-Site Scripting Attacks - SecurityTracker
rhn.redhat.com | Red Hat Support
Mozilla Firefox Multiple Vulnerabilities - Advisories - Secunia
Ubuntu update for firefox - Advisories - Secunia
IBM X-Force Exchange
USN-490-1: Firefox vulnerabilities | Ubuntu
SecurityFocus
Debian -- Security Information -- DSA-1338-1 iceweasel
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 registred 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**