



# CVE-2014-1574

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

## Summary

|                        |                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2014-1574                                                                                                                  |
| <b>State</b>           | PUBLIC                                                                                                                         |
| <b>Assigner</b>        | security@mozilla.org                                                                                                           |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                   |
| <b>Published</b>       | 2014-10-15 10:55:00 UTC                                                                                                        |
| <b>Updated</b>         | 2016-12-24 02:59:00 UTC                                                                                                        |
| <b>Description</b>     | Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 33.0, Firefox ESR 31.x before 31.2, and 7 |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                  | Product                     | Version | Update | Edition | Language |
|-------------|-------------------------|-----------------------------|---------|--------|---------|----------|
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 30.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 31.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 31.1.0  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 30.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 31.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 31.1.0  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | All     | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox ESR</a> | 31.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox ESR</a> | 31.1.0  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox ESR</a> | 31.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox ESR</a> | 31.1.0  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 31.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 31.1.0  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 31.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 31.1.0  | All    | All     | All      |

## References

| Reference                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------|
| Access Denied                                                                                                                              |
| Access Denied                                                                                                                              |
| 1011354 – crash in mozilla::net::nsHttpChannel::OnStopRequest(nsIRequest*, nsISupports*, tag_nsresult)                                     |
| Access Denied                                                                                                                              |
| Gentoo Security                                                                                                                            |
| [SECURITY] Fedora 21 Update: firefox-33.0-1.fc21                                                                                           |
| Security Advisory SA62021 - SUSE update for MozillaThunderbird - Secunia                                                                   |
| [security-announce] openSUSE-SU-2015:1266-1: important: Mozilla (Firefox                                                                   |
| openSUSE-SU-2014:1346-1: moderate: update for MozillaThunderbird                                                                           |
| Access Denied                                                                                                                              |
| Debian -- Security Information -- DSA-3050-1 iceweasel                                                                                     |
| Mozilla Firefox Bugs Let Remote Users Execute Arbitrary Code, Bypass Same Origin-Policy, and Obtain Potentially Sensitive Information - Se |
| Mozilla Firefox/Thunderbird CVE-2014-1574 Multiple Memory Corruption Vulnerabilities                                                       |
| Red Hat Customer Portal                                                                                                                    |
| [SECURITY] Fedora 20 Update: firefox-33.0-1.fc20                                                                                           |
| Mozilla Thunderbird Bugs Let Remote Users Execute Arbitrary Code - SecurityTracker                                                         |
| Access Denied                                                                                                                              |
| openSUSE-SU-2014:1344-1: moderate: update for firefox, mozilla-nspr, moz                                                                   |
| Mageia Advisory: MGASA-2014-0421 - Updated firefox and thunderbird packages fix security vulnerabilities                                   |
| Security Advisory SA61387 - Debian update for icedove - Secunia                                                                            |
| [security-announce] openSUSE-SU-2015:0138-1: important: Firefox update t                                                                   |
| Security Advisory SA62023 - SUSE update for firefox, mozilla-nspr, and mozilla-nss - Secunia                                               |
| Red Hat Customer Portal                                                                                                                    |
| Miscellaneous memory safety hazards (rv:33.0 / rv:31.2) — Mozilla                                                                          |
| USN-2373-1: Thunderbird vulnerabilities   Ubuntu                                                                                           |
| Security Advisory SA61854 - Mageia update for firefox and thunderbird - Secunia                                                            |
| openSUSE-SU-2014:1343-1: moderate: update for MozillaThunderbird                                                                           |
| openSUSE-SU-2014:1345-1: moderate: update for firefox, mozilla-nspr, moz                                                                   |
| Debian -- Security Information -- DSA-3061-1 icedove                                                                                       |
| Security Advisory SA62022 - SUSE update for firefox, mozilla-nspr, mozilla-nss, and seamonkey - Secunia                                    |
| USN-2372-1: Firefox vulnerabilities   Ubuntu                                                                                               |
| Oracle Solaris Third Party Bulletin - April 2015                                                                                           |
| 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](#)