



# CVE-2015-2724

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

## Summary

|                        |                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2015-2724                                                                                                                 |
| <b>State</b>           | PUBLIC                                                                                                                        |
| <b>Assigner</b>        | security@mozilla.org                                                                                                          |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                  |
| <b>Published</b>       | 2015-07-06 02:00:00 UTC                                                                                                       |
| <b>Updated</b>         | 2023-09-12 14:55:00 UTC                                                                                                       |
| <b>Description</b>     | Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 3 |

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                    | Product                      | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 12.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 15.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 12.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 15.04   | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 8.0     | 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    | 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>  | 31.1.1  | All    | All     | All      |

|                  |         |                                                |        |     |     |     |
|------------------|---------|------------------------------------------------|--------|-----|-----|-----|
|                  |         |                                                |        |     |     |     |
| Application      | Mozilla | Firefox Esr                                    | 31.2   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.3   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.3.0 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.4   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.5   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.5.1 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.5.2 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.5.3 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.6.0 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.7.0 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 38.0   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.0   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.1   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.1.0 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.1.1 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.2   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.3   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.3.0 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.4   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.5   | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.5.1 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.5.2 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.5.3 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.6.0 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 31.7.0 | All | All | All |
| Application      | Mozilla | Firefox Esr                                    | 38.0   | All | All | All |
| Application      | Mozilla | Thunderbird                                    | All    | All | All | All |
| Operating System | Novell  | Suse Linux Enterprise Desktop                  | 12.0   | All | All | All |
| Operating System | Novell  | Suse Linux Enterprise Desktop                  | 12.0   | All | All | All |
| Operating System | Novell  | Suse Linux Enterprise Server                   | 11     | sp4 | All | All |
| Operating System | Novell  | Suse Linux Enterprise Server                   | 12.0   | All | All | All |
| Operating System | Novell  | Suse Linux Enterprise Server                   | 11     | sp4 | All | All |
| Operating System | Novell  | Suse Linux Enterprise Server                   | 12.0   | All | All | All |
| Application      | Novell  | Suse Linux Enterprise Software Development Kit | 12.0   | All | All | All |
| Operating System | Novell  | Suse Linux Enterprise Software Development Kit | 12.0   | All | All | All |

|                  |                        |                                                                |      |     |     |     |
|------------------|------------------------|----------------------------------------------------------------|------|-----|-----|-----|
| Operating System | <a href="#">Novell</a> | <a href="#">Suse Linux Enterprise Software Development Kit</a> | 12.0 | All | All | All |
| Operating System | <a href="#">Oracle</a> | <a href="#">Solaris</a>                                        | 11.3 | All | All | All |
| Operating System | <a href="#">Oracle</a> | <a href="#">Solaris</a>                                        | 11.3 | All | All | All |

References

| Reference                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Oracle Solaris Bulletin - April 2016                                                                                                          |
| [security-announce] openSUSE-SU-2015:1229-1: important: Security update                                                                       |
| Debian -- Security Information -- DSA-3300-1 iceweasel                                                                                        |
| Red Hat Customer Portal                                                                                                                       |
| [security-announce] SUSE-SU-2015:1268-1: important: Security update for                                                                       |
| Red Hat Customer Portal                                                                                                                       |
| USN-2656-2: Firefox vulnerabilities   Ubuntu                                                                                                  |
| [security-announce] openSUSE-SU-2015:1266-1: important: Mozilla (Firefox                                                                      |
| USN-2673-1: Thunderbird vulnerabilities   Ubuntu                                                                                              |
| Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restriction |
| Oracle Solaris Third Party Bulletin - October 2015                                                                                            |
| [security-announce] SUSE-SU-2015:1269-1: important: Security update for                                                                       |
| Debian -- Security Information -- DSA-3324-1 icedove                                                                                          |
| [security-announce] SUSE-SU-2015:1449-1: important: Security update for                                                                       |
| Access Denied                                                                                                                                 |
| Access Denied                                                                                                                                 |
| Access Denied                                                                                                                                 |
| USN-2656-1: Firefox vulnerabilities   Ubuntu                                                                                                  |
| Miscellaneous memory safety hazards (rv:39.0 / rv:31.8 / rv:38.1) — Mozilla                                                                   |
| Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security                                                                 |
| Access Denied                                                                                                                                 |
| Mozilla Thunderbird Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Bypass Security F   |
| Mozilla Firefox/Thunderbird Multiple Security Vulnerabilities                                                                                 |
| 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](#)