# CVE-2015-2712

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2015-2712 |
| **State** | PUBLIC |
| **Assigner** | security@mozilla.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2015-05-14 10:59:00 UTC |
| **Updated** | 2018-10-30 16:27:00 UTC |
| **Description** | The asm.js implementation in Mozilla Firefox before 38.0 does not properly determine heap lengths during identification of c |

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Mozilla | Firefox | All | All | All | All |
| Operating System | Opensuse | Opensuse | 13.1 | All | All | All |
| Operating System | Opensuse | Opensuse | 13.2 | All | All | All |
| Operating System | Opensuse | Opensuse | 13.1 | All | All | All |
| Operating System | Opensuse | Opensuse | 13.2 | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| Oracle Solaris Bulletin - April 2016 | CONFIRM | www.oracle.com | |
| Out-of-bounds read and write in asm.js validation — Mozilla | CONFIRM | www.mozilla.org | Vendor Advisory |
| Mozilla Firefox and Thunderbird MFSA 2015-48 through -58 Multiple Vulnerabilities | BID | www.securityfocus.com | |
| Access Denied | CONFIRM | bugzilla.mozilla.org | |
| Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security | GENTOO | security.gentoo.org | |
| openSUSE-SU-2015:0934-1: moderate: Security update for MozillaFirefox | SUSE | lists.opensuse.org | |
| USN-2602-1: Firefox vulnerabilities \| Ubuntu | UBUNTU | www.ubuntu.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analys |

No vendor comments have been submitted for 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**