# CVE-2015-7197

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2015-7197 |
| **State** | PUBLISHED |
| **Assigner** | mozilla |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2015-11-05 05:59:21 UTC |
| **Updated** | 2026-05-06 22:30:45 UTC |
| **Description** | Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 improperly control the ability of a web worker to create a Web |

## Risk And Classification

**Primary CVSS:** v2.0 5 from nvd@nist.gov

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

**Problem Types:** CWE-264 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/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 | 38.0 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Mozilla | Firefox | 38.0.1 | All | All | All |
| Application | Mozilla | Firefox | 38.0.5 | All | All | All |
| Application | Mozilla | Firefox | 38.1.0 | All | All | All |
| Application | Mozilla | Firefox | 38.1.1 | All | All | All |
| Application | Mozilla | Firefox | 38.2.0 | All | All | All |
| Application | Mozilla | Firefox | 38.2.1 | All | All | All |
| Application | Mozilla | Firefox | 38.3.0 | All | All | All |
| Application | Mozilla | Firefox | All | All | All | All |

## Vendor Declared Affected Products

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

## References

| Reference |
|---|
| [security-announce] SUSE-SU-2015:1978-1: important: Security update for |
| Mozilla Firefox Multiple Security Vulnerabilities |
| Mixed content WebSocket policy bypass through workers — Mozilla |
| [security-announce] openSUSE-SU-2015:1942-1: important: Security update |
| 1204269 - (CVE-2015-7197) WebSocket secure requirements can be bypassed in a worker |
| Red Hat Customer Portal |
| Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restriction |
| [security-announce] SUSE-SU-2015:1926-1: important: Security update for |
| Debian -- Security Information -- DSA-3393-1 iceweasel |
| openSUSE-SU-2015:2245-1: moderate: Security update for Mozilla Thunderbi |
| USN-2785-1: Firefox vulnerabilities \| Ubuntu |
| Debian -- Security Information -- DSA-3410-1 icedove |
| Red Hat Customer Portal |
| [security-announce] SUSE-SU-2015:2081-1: important: Security update for |
| openSUSE-SU-2015:2229-1: moderate: Security update for MozillaThunderbir |
| Oracle Linux Bulletin - October 2015 |
| [security-announce] SUSE-SU-2015:1981-1: important: Security update for |
| USN-2819-1: Thunderbird vulnerabilities \| Ubuntu |
| Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security |
| Oracle Solaris Bulletin - April 2016 |
| CVE Program record |
| NVD vulnerability detail |

NVD vulnerability detail

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**