# CVE-2016-1667

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-1667 |
| **State** | PUBLIC |
| **Assigner** | security@google.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2016-05-14 21:59:00 UTC |
| **Updated** | 2023-11-07 02:30:00 UTC |
| **Description** | The TreeScope::adoptIfNeeded function in WebKit/Source/core/dom/TreeScope.cpp in the DOM implementation in Blink, a |

## Risk And Classification

**Problem Types:** CWE-284

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Application | Google | Chrome | All | All | All | All |
| Operating System | Opensuse | Opensuse | 13.1 | All | All | All |
| Operating System | Opensuse | Opensuse | 13.1 | All | All | All |

## References

| Reference |
|---|
| USN-2960-1: Oxide vulnerabilities \| Ubuntu |
| [security-announce] openSUSE-SU-2016:1319-1: important: Security update |
| 605766 - chromium - An open-source project to help move the web forward. - Monorail |
| Chrome Releases: Stable Channel Update |
| [security-announce] openSUSE-SU-2016:1655-1: important: Security update |
| Issue 1953323002: Don't allow scripts to run when a node is being adopted. - Code Review |
| Chromium: Multiple vulnerabilities (GLSA 201605-02) — Gentoo security |
| Google Chrome Prior to 50.0.2661.102 Multiple Security Vulnerabilities |
| [security-announce] openSUSE-SU-2016:1304-1: important: Security update |

| |
|---|
| Debian -- Security Information -- DSA-3590-1 chromium-browser |
| Red Hat Customer Portal |
| Google Chrome Multiple Flaws Lets Remote Users Bypass Same-Origin Restrictions, Traverse the Directory, and Execute Arbitrary Code - Se |
| 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.