# CVE-2016-1647

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-1647 |
| **State** | PUBLISHED |
| **Assigner** | Chrome |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2016-03-29 10:59:01 UTC |
| **Updated** | 2026-05-06 22:30:45 UTC |
| **Description** | Use-after-free vulnerability in the RenderWidgetHostImpl::Destroy function in content/browser/renderer_host/render_widget |

## Risk And Classification

**Primary CVSS:** v3.0 8.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**Problem Types:** NVD-CWE-Other | n/a

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.0 | nvd@nist.gov | Primary | 8.8 | HIGH | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 2.0 | nvd@nist.gov | Primary | 9.3 | | AV:N/AC:M/Au:N/C:C/I:C/A:C |

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 15.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | 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 |

## Vendor Declared Affected Products

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

## References

| Reference | Source |
|---|---|
| [security-announce] openSUSE-SU-2016:0930-1: important: Security update | af854a3a-2127-422b-91a |
| 590284 - Security: RWHI UaF from bad fullscreen widget routing id - chromium - Monorail | af854a3a-2127-422b-91a |
| Chromium: Multiple vulnerabilities (GLSA 201605-02) — Gentoo security | af854a3a-2127-422b-91a |
| Red Hat Customer Portal | af854a3a-2127-422b-91a |
| Issue 1747183002: Check that RWHI isn't deleted manually while owned by a scoped_ptr in RVHI - Code Review | af854a3a-2127-422b-91a |

| | |
|---|---|
| [security-announce] openSUSE-SU-2016:1059-1: important: Security update | af854a3a-2127-422b-91a |
| USN-2955-1: Oxide vulnerabilities \| Ubuntu | af854a3a-2127-422b-91a |
| Google Chrome Multiple Flaws Lets Remote Users Execute Arbitrary Code - SecurityTracker | af854a3a-2127-422b-91a |
| Debian -- Security Information -- DSA-3531-1 chromium-browser | af854a3a-2127-422b-91a |
| Chrome Releases: Stable Channel Update | af854a3a-2127-422b-91a |
| Issue 1811783002: Disallow was_within_same_page = true for a cross-process navigation. - Code Review | af854a3a-2127-422b-91a |
| [security-announce] openSUSE-SU-2016:0929-1: important: Security update | af854a3a-2127-422b-91a |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

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**