CVE-2016-1680

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

Summary

CVE	CVE-2016-1680
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-05 23:59:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Use-after-free vulnerability in ports/SkFontHost_FreeType.cpp in Skia, as used in Google Chrome before 51.0.2704.63, allc

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: CWE-119 | 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	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

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

Partial

Integrity

Partial

Availability

Partial

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

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	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Suse	Linux Enterprise	12.0	All	All	All

Vendor Declared Affected Products

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

References

Reference

Debian -- Security Information -- DSA-3590-1 chromium-browser
Issue 589848 - chromium - An open-source project to help move the web forward. - Monorail
Issue 1751883004: SkFontHost_FreeType constructor to correctly release resources. - Code Review
[security-announce] openSUSE-SU-2016:1430-1: important: Security update
Chrome Releases: Stable Channel Update
Google Chrome Prior to 51.0.2704.63 Multiple Security Vulnerabilities
Chromium: Multiple vulnerabilities (GLSA 201607-07) — Gentoo security
[security-announce] openSUSE-SU-2016:1433-1: important: Security update
Red Hat Customer Portal
[security-announce] openSUSE-SU-2016:1496-1: important: Security update
Google Chrome Multiple Flaws Lets Remote Users Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information, and Execute A
USN-2992-1: Oxide vulnerabilities | Ubuntu
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.