



CVE-2016-1649

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

Summary

CVE	CVE-2016-1649
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-03-29 10:59:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Program::getUniformInternal function in Program.cpp in libANGLE, as used in Google Chrome before 49.0.2623.108, c

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	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-91ae-364da2661108
595836 - libANGLE buffer-overflow (part of pwn2own exploit) - chromium - Monorail	af854a3a-2127-422b-91ae-364da2661108
Chromium: Multiple vulnerabilities (GLSA 201605-02) — Gentoo security	af854a3a-2127-422b-91ae-364da2661108
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108
[security-announce] openSUSE-SU-2016:1059-1: important: Security update	af854a3a-2127-422b-91ae-364da2661108

USN-2955-1: Oxide vulnerabilities Ubuntu	af854a3a-2127-422b-91ae-364da2661108	v
Google Chrome Multiple Flaws Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da2661108	v
chromium-review.googlesource.com/334448	af854a3a-2127-422b-91ae-364da2661108	c
Zero Day Initiative	af854a3a-2127-422b-91ae-364da2661108	v
Debian -- Security Information -- DSA-3531-1 chromium-browser	af854a3a-2127-422b-91ae-364da2661108	v
Chrome Releases: Stable Channel Update	af854a3a-2127-422b-91ae-364da2661108	c
[security-announce] openSUSE-SU-2016:0929-1: important: Security update	af854a3a-2127-422b-91ae-364da2661108	li
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.