CVE-2016-5190

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

Summary

CVE	CVE-2016-5190
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-18 03:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object life

Risk And Classification

Primary CVSS: v3.0 6.3 MEDIUM from nvd@nist.gov

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

EPSS: 0.006130000 probability, percentile 0.699520000 (date 2026-05-10)

Problem Types: CWE-416 | out of bounds memory read

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	6.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
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

Low

Integrity

Low

Availability

Low

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

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
Application	Google	Chrome	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Na	Chrome Prior To 54.0.2840.59 For Windows Mac And Linux 54.0.2840.85 For Android	affected Chrome prior to 54.0.28

References

Reference	Sour
Chromium: Multiple vulnerabilities (GLSA 201610-09) — Gentoo security	af854
642067 - Heap-use-after-free in base::ObserverListBase<content::RenderThreadObserver>::RemoveObserver - chromium - Monorail	af854
Chrome Releases: Stable Channel Update for Desktop	af854
Red Hat Customer Portal	af854
Google Chrome Prior to 54.0.2840.59 Multiple Security Vulnerabilities	af854
CVE Program record	CVE.
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**