CVE-2026-6313

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

Summary

CVE	CVE-2026-6313
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 20:16:41 UTC
Updated	2026-04-17 17:26:05 UTC
Description	Insufficient policy enforcement in CORS in Google Chrome prior to 147.0.7727.101 allowed a remote attacker who had com

Risk And Classification

Primary CVSS: v3.1 3.1 LOW from ADP

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

EPSS: 0.000090000 probability, percentile 0.008800000 (date 2026-04-20)

Problem Types: CWE-284 | Insufficient policy enforcement | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Google	Chrome	affected 147.0.7727.101 147.0.7727.101 custom	Not specified

References

Reference	Source	Link
chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_15.html	chrome-cve-admin@google.com	chromereleases.go
issues.chromium.org/issues/498765210	chrome-cve-admin@google.com	issues.chromium.o
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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