

CVE-2017-5070

Google Chromium V8 Type Confusion Vulnerability

CISA KEV since Jun 8, 2022

Actively exploited

Type confusion in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.321 98.3rd percentile · FIRST	CISA DEADLINE Jun 22, 2022 KEV since 2022 · listed over a year
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.321 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
chrome	< 59.0.3071.86 < 59.0.3071.92	59.0.3071.86 · 59.0.3071.92	NVD
macos	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
android	—	no fixed version listed	NVD
enterprise linux desktop	6.0	no fixed version listed	NVD
enterprise linux server	6.0	no fixed version listed	NVD
enterprise linux workstation	6.0	no fixed version listed	NVD

Sources

Vendor guidance access.redhat.com/errata/RHSA-2017:1399

Additional guidance chromereleases.googleblog.com/2017/06/stable-channel-update-for-desktop.html

Additional guidance security.gentoo.org/glsa/201706-20

NVD

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD

Current data evulnable.com/vulnerability-management/cve/CVE-2017-5070

nvd.nist.gov/vuln/detail/CVE-2017-5070
euvd.enisa.europa.eu/vulnerability/EUVD-2017-14179

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.