



CVE-2018-17463

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2018-17463 |
| State | PUBLIC |
| Assigner | chrome-cve-admin@google.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-11-14 15:29:00 UTC |
| Updated | 2020-08-24 17:37:00 UTC |
| Description | Incorrect side effect annotation in V8 in Google Chrome prior to 70.0.3538.64 allowed a remote attacker to execute arbitrary code with system privileges. |

Risk And Classification

EPSS: 0.921990000 probability, percentile 0.997110000 (date 2026-04-01)

CISA KEV: Listed on 2022-06-08; due 2022-06-22; ransomware use Unknown

Problem Types: NVD-CWE-noinfo

CISA Known Exploited Vulnerability

| | |
|------------------------|---|
| Vendor | Google |
| Product | Chromium V8 |
| Name | Google Chromium V8 Remote Code Execution Vulnerability |
| Required Action | Apply updates per vendor instructions. |
| Notes | https://nvd.nist.gov/vuln/detail/CVE-2018-17463 |

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|------------------------|-------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Google | Chrome | All | All | All | All |
| Application | Google | Chrome | All | All | All | All |
| Operating System | Redhat | Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Linux Server | 6.0 | All | All | All |

| | | | | | | |
|------------------|------------------------|-----------------------------------|-----|-----|-----|-----|
| Operating System | Redhat | Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Linux Workstation | 6.0 | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|--|------------------|
| Debian -- Security Information -- DSA-4330-1 chromium-browser | DEBIAN | www.debian.org | Third Party Adv |
| Red Hat Customer Portal | REDHAT | access.redhat.com | Third Party Adv |
| Google Chrome 67 / 68 / 69 Object.create Type Confusion ≈ Packet Storm | MISC | packetstormsecurity.com | |
| Chromium: Multiple vulnerabilities (GLSA 201811-10) — Gentoo security | GENTOO | security.gentoo.org | Third Party Adv |
| 888923 - Security: Chrome RCE - chromium - Monorail | MISC | crbug.com | Permissions Re |
| Chrome Releases: Stable Channel Update for Desktop | CONFIRM | chromereleases.googleblog.com | Release Notes, |
| Google Chrome Prior to 70.0.3538.67 Multiple Security Vulnerabilities | BID | www.securityfocus.com | Third Party Adv |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analy |
| CISA Known Exploited Vulnerabilities catalog | CISA | www.cisa.gov | kev |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710206](#) Gentoo Linux Chromium Multiple Vulnerabilities (GLSA 201811-10)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report