



CVE-2019-5763

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2019-5763 |
| State | PUBLIC |
| Assigner | security@google.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-02-19 17:29:00 UTC |
| Updated | 2023-11-07 03:11:00 UTC |
| Description | Failure to check error conditions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit |

Risk And Classification

Problem Types: CWE-754

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 |
| Operating System | Fedoraproject | Fedora | 29 | All | All | All |
| Operating System | Fedoraproject | Fedora | 30 | All | All | All |
| Operating System | Fedoraproject | Fedora | 29 | All | All | All |
| Operating System | Fedoraproject | Fedora | 30 | All | All | All |
| Application | Google | Chrome | All | All | All | All |
| Application | Google | Chrome | All | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |

References

| Reference | Source | Link |
|-----------|--------|------|
|-----------|--------|------|

| | | |
|---|---------|--|
| Debian -- Security Information -- DSA-4395-1 chromium | | www.debian.org |
| 914731 - chromium - An open-source project to help move the web forward. - Monorail | MISC | crbug.com |
| Chrome Releases: Stable Channel Update for Desktop | | chromereleases.googleusercontent.com |
| Google Chrome Prior to 72.0.3626.81 Multiple Security Vulnerabilities | | www.securityfocus.com |
| [SECURITY] Fedora 30 Update: chromium-73.0.3683.75-2.fc30 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| [SECURITY] Fedora 29 Update: chromium-73.0.3683.75-2.fc29 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| [SECURITY] Fedora 30 Update: chromium-73.0.3683.75-2.fc30 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| [SECURITY] Fedora 29 Update: chromium-73.0.3683.75-2.fc29 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| Red Hat Customer Portal | | access.redhat.com |
| 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.

© [CVE.report](http://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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org). This site includes MITRE data granted under the following [license](http://www.mitre.org).

Free CVE JSON API cve.report/api

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