



CVE-2018-6123

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2018-6123 |
| State | PUBLIC |
| Assigner | security@google.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-01-09 19:29:00 UTC |
| Updated | 2023-11-07 02:59:00 UTC |
| Description | A use after free in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corrup |

Risk And Classification

Problem Types: CWE-787 | CWE-416

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 | 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

[Debian -- Security Information -- DSA-4237-1 chromium-browser](#)

[Google Chrome Prior to 67.0.3396.62 Multiple Security Vulnerabilities](#)

[835639 - chromium - An open-source project to help move the web forward. - Monorail](#)

[Google Chrome Multiple Flaws Let Remote Bypass Security Restrictions, Spoof URLs, Obtain Potentially Sensitive Information, and Execute /](#)

Chrome Releases: Stable Channel Update for Desktop

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

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

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

Free CVE JSON API cve.report/api

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