



# CVE-2016-5178

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

## Summary

<b>CVE</b>	CVE-2016-5178
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-23 04:29:00 UTC
<b>Updated</b>	2023-11-07 02:33:00 UTC
<b>Description</b>	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.143 allow remote attackers to cause a denial of ser

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	25	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	25	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Supplementary</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Supplementary</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation Supplementary</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation Supplementary</a>	6.0	All	All	All

## References

## Reference

Google Chrome Prior to 52.0.2743.82 Multiple Security Vulnerabilities

645028 - Web accessible resources checks should work with blob: and filesystem: URLs that have chrome-extension:// inner URLs - chromium

[SECURITY] Fedora 25 Update: chromium-53.0.2785.143-1.fc25 - package-announce - Fedora Mailing-Lists

Chromium: Multiple vulnerabilities (GLSA 201610-09) — Gentoo security

openSUSE-SU-2016:2429-1: moderate: Security update for chromium

Red Hat Customer Portal

Debian -- Security Information -- DSA-3683-1 chromium-browser

openSUSE-SU-2016:2432-1: moderate: Security update for chromium

[SECURITY] Fedora 24 Update: chromium-53.0.2785.143-1.fc24 - package-announce - Fedora Mailing-Lists

Chrome Releases: Stable Channel Update for Desktop

[SECURITY] Fedora 25 Update: chromium-53.0.2785.143-1.fc25 - package-announce - Fedora Mailing-Lists

651092 - Tracking bug for internal fixes: Chrome M53, release 3 - chromium - Monorail

Google Chrome Use-After-Free Memory Error and Other Bugs Let Remote Users Execute Arbitrary Code - SecurityTracker

1380632 – (CVE-2016-5178) CVE-2016-5178 chromium-browser: various fixes from internal audits

[SECURITY] Fedora 24 Update: chromium-53.0.2785.143-1.fc24 - package-announce - Fedora Mailing-Lists

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](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)