



CVE-2016-1637

Published on: 03/05/2016 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:30:00 AM UTC

CVE-2016-1637

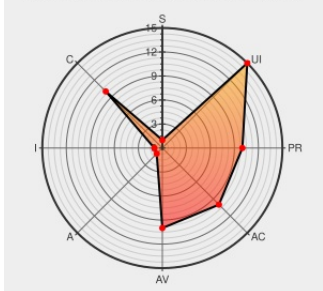
[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N



Certain versions of [Chrome](#) from [Google](#) contain the following vulnerability:

The SkATan2_255 function in effects/gradients/SkSweepGradient.cpp in Skia, as used in Google Chrome before 49.0.2623.75, mishandles arctangent calculations, which allows remote attackers to obtain sensitive information via a crafted web site.

CVE-2016-1637 has been assigned by [Google](#) security@google.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2016:0684-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0684
Google Chrome Prior to 49.0.2623.75 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 84008

USN-2920-1: Oxide vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2920-1
[security-announce] openSUSE-SU-2016:0664-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0664
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201603-09
Debian -- Security Information -- DSA-3507-1 chromium-browser	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3507
555544 - crash in SkSweepGradient::SweepGradientContext::shadeSpan - chromium - Monorail	code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=555544
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Obtain Potentially Sensitive Information - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1035185
Issue 1506913002: Pin result in SkATan2_255 - Code Review	codereview.chromium.org text/html	 CONFIRM codereview.chromium.org/1506913002
[security-announce] openSUSE-SU-2016:0729-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0729
[security-announce] SUSE-SU-2016:0665-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:0665
Chrome Releases: Stable Channel Update	googlechromereleases.blogspot.com text/html	 CONFIRM googlechromereleases.blogspot.com/2016/03/schannel-update.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All
cpe:2.3:a:google:chrome:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)