



CVE-2015-6781

Published on: 12/05/2015 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:27:00 AM UTC

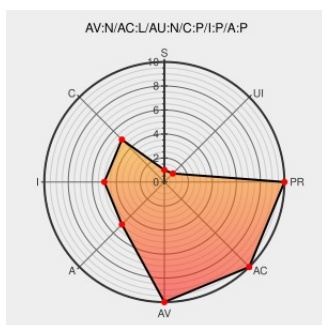
CVE-2015-6781

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Integer overflow in the `FontData::Bound` function in `data/font_data.cc` in Google sfntly, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted offset or length value within font data in an SFNT container.

CVE-2015-6781 has been assigned by [Google](#) security@google.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

[security-announce]
openSUSE-SU-2015:2291-1: important: Security update

[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2015:2291](#)

Google Chrome Prior to 47.0.2526.73 Multiple Security Vulnerabilities

[cve.report \(archive\)](#)
[text/html](#)

[BID 78416](#)

Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security

[security.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-201603-09](#)

Chrome Releases: Stable

[googlechromereleases.blogspot.com](#)

[CONFIRM googlechromereleases.blogspot.com/2015/12/stable-channel-releases.html](#)

Channel Update	text/html	update.html
Debian -- Security Information -- DSA-3415-1 chromium-browser	www.debian.org Deprecated Link text/html	DEBIAN DSA-3415
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Spoof Content - SecurityTracker	www.securitytracker.com text/html	SECTrack 1034298
Issue 1367323002: Pull sfntly from GitHub instead of code.google.com. - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1367323002/
Check for integer overflow in sfntly::FontData::Bound(). . googlei18n/sfntly@de776d4 · GitHub	github.com text/html	CONFIRM github.com/googlei18n/sfntly/commit/de776d4ef06ca29c240de3444348894
Issue 497302 - chromium - Integer-overflow in sfntly::FontData::Bound - ???? ** Chromium issue tracking will soon migrate to https://bugs.chromium.org (Monorail) ** ???? - Google Project Hosting	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=497302
[security-announce] openSUSE-SU-2015:2290- 1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2290

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 →](#)

© [CVE.report](#) 2023   |

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](#)