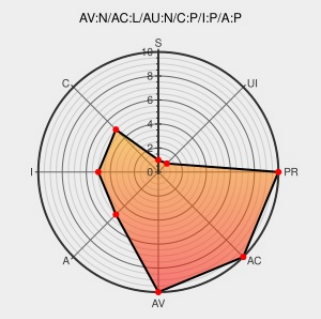
CVE-2015-6781

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 security@google.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	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-channe

Channel Update	text/html	update.html
Debian -- Security Information -- DSA-3415-1 chromium-browser	www.debian.org Depreciated 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/de776d4ef06ca29c240de344434889
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

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 and Source URL Uptime Status status.cve.report