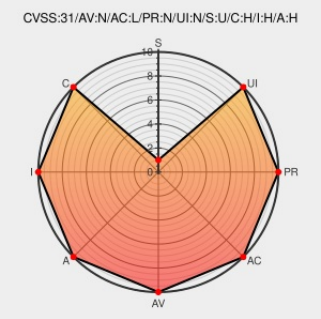
CVE-2015-6764

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

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

CVE-2015-6764

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

The BasicJsonStringifier::SerializeJSArray function in json-stringifier.h in the JSON stringifier in Google V8, as used in Google Chrome before 47.0.2526.73, improperly loads array elements, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2015-6764 has been assigned by security@google.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

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
Chromium: Multiple vulnerabilities (GLSA	security.gentoo.org	GENTOO GLSA-201603-09

Chromium: Multiple Vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA 201603-09
Chrome Releases: Stable Channel Update	googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/20 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
openSUSE-SU-2016:0138-1: moderate: Security update for nodejs	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0138
Issue 554946 - chromium - Security: Pwn2Own mobile case, out-of-bound access in json stringifier - ???? ** 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/det
6df9a1db8c85ab63dee63879456b6027df53fabc - v8/v8 - Git at Google	chromium.googlesource.com text/html	CONFIRM chromium.googlesource.com/v8/v8/+/6df9a1db8c85ab
Node.js CVE-2015-6764 Out of Bounds Denial of Service Vulnerability	cve.report (archive) text/html	BID 78209
Issue 1440223002: [JSON stringifier] reintroduce fast path with bail out to slow path. - Code Review	codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1440223002
[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
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:a:nodejs:node.js:*:*:*:*:lts:*:*:*:

cpe:2.3:a:nodejs:node.js:*:*:*:*:-:*:*:*:

cpe:2.3:a:nodejs:node.js:*:*:*:*:-:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→