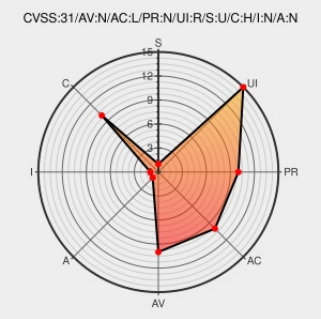
CVE-2016-5172

Published on: 09/25/2016 12:00:00 AM UTC

Last Modified on: 08/29/2022 08:43:00 PM UTC

CVE-2016-5172

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



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

The parser in Google V8, as used in Google Chrome before 53.0.2785.113, mishandles scopes, which allows remote attackers to obtain sensitive information from arbitrary memory locations via crafted JavaScript code.

CVE-2016-5172 has been assigned by 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
Chromium: Multiple vulnerabilities (GLSA 201610-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201610-09
Issue 2077283004: Rewrite scopes of non-simple default arguments - Code Review	Issue Tracking Patch	CONFIRM codereview.chromium.org/2077283004

	codereview.chromium.org text/html	
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1905
Chrome Releases: Stable Channel Update for Desktop	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2016/09/stable-channel-update-for-desktop_13.html
616386 - Security: Arbitrary Memory Read in v8 - chromium - Monorail	Permissions Required crbug.com text/html	CONFIRM crbug.com/616386
Debian -- Security Information -- DSA-3667-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3667
Google Chrome Prior to 53.0.2785.113 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 92942
Google Chrome Multiple Flaws Lets Remote Users Obtain Potentially Sensitive Information and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036826

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

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:*:*:*:*:-:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report