



CVE-2020-6485

Published on: 05/20/2020 12:00:00 AM UTC

Last Modified on: 10/05/2022 07:29:00 PM UTC

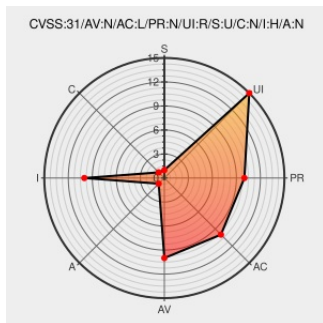
CVE-2020-6485

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Insufficient data validation in media router in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.

CVE-2020-6485 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Google - Chrome** version < 83.0.4103.61

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	NONE	HIGH	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Chromium, Google Chrome: Multiple vulnerabilities (GL SA 202006-02) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202006-02

[SECURITY] Fedora 31 Update: chromium-83.0.4103.116-3.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-77f89ab772
Debian -- Security Information -- DSA-4714-1 chromium	www.debian.org Deprecated Link text/html	 DEBIAN DSA-4714
[security-announce] openSUSE-SU-2020:0823-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:0823
1047285 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Vendor Advisory cbug.com text/html	 MISC cbug.com/1047285
Chrome Releases: Stable Channel Update for Desktop	Release Notes Vendor Advisory chromereleases.googleblog.com text/html	 MISC chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop_19.html
[SECURITY] Fedora 32 Update: chromium-83.0.4103.116-3.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-08561721ad
[security-announce] openSUSE-SU-2020:0832-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:0832
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
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Google	Chrome Os	-	All	All	All
Operating System	Google	Chrome Os	-	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All

Operating System

Opensuse

Leap

15.1

All

All

All

cpe:2.3:o:debian:debian_linux:10.0:*****:

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

cpe:2.3:o:fedoraproject:fedora:31:*****:

cpe:2.3:o:fedoraproject:fedora:32:*****:

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

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

cpe:2.3:o:google:chrome_os:-:*****:

cpe:2.3:o:google:chrome_os:-:*****:

cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*****:

cpe:2.3:o:opensuse:leap:15.1:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ?? Insufficient data validation in media ro... CVE-2020-6485 Link for more: alerts.remotelyrmm.com/CVE-2020-6485	2022-10-05 21:32:15

← Previous ID

Next ID →