



CVE-2020-6566

Published on: 09/21/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:24:00 AM UTC

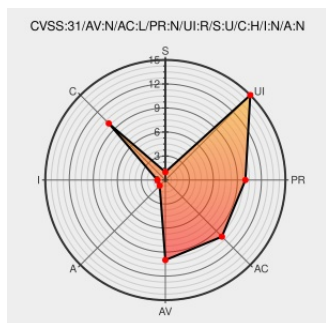
CVE-2020-6566

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Insufficient policy enforcement in media in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.

CVE-2020-6566 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Google - Chrome** version < 85.0.4183.83

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
[security-announce] openSUSE-SU-2020:1514-1: important: Security update	Third Party Advisory lists.opensuse.org	SUSE openSUSE-SU-2020:1514

important: Security update	lists.opensuse.org text/html	
[security-announce] openSUSE-SU-2020:1510-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:1510
1065264 - chromium - An open-source project to help move the web forward. - Monorail	Permissions Required Vendor Advisory crlbug.com text/html	 MISC crbug.com/1065264
[SECURITY] Fedora 33 Update: chromium- 85.0.4183.83-1.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-6da740d38c
Debian -- Security Information -- DSA-4824-1 chromium	www.debian.org Deprecated Link text/html	 DEBIAN DSA-4824
Chrome Releases: Stable Channel Update for Desktop	Release Notes Vendor Advisory chromereleases.googleblog.com text/html	 MISC chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop_25.html
[security-announce] openSUSE-SU-2020:1499-1: important: Security update	Mailing List Patch Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:1499
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.		

Related QID Numbers

[690503](#) Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (d73bc4e6-e7c4-11ea-a878-e09467587c17)

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	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Application	Opensuse	Backports Sle	15.0	sp2	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Application	Opensuse	Backports Sle	15.0	sp2	All	All

Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:						
cpe:2.3:a:google:chrome:*:*:*:*:*:						
cpe:2.3:a:google:chrome:*:*:*:*:*:						
cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:						
cpe:2.3:a:opensuse:backports_sle:15.0:sp2:*:*:*:*:						
cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:						
cpe:2.3:a:opensuse:backports_sle:15.0:sp2:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.2:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.2:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← Previous ID Next ID→		