

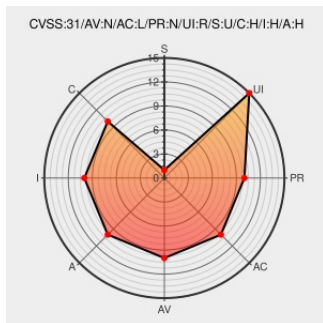


CVE-2020-6551

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

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-6551

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Use after free in WebXR in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-6551 has been assigned by [chrome-cve-admin@google.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Google](#) - **Chrome** version < **84.0.4147.125**

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **9.3 - HIGH**

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

CVE References

Description	Tags	Link
Chrome Releases: Stable Channel Update for Desktop	Release Notes Vendor Advisory chromereleases.googleblog.com	MISC chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop.html

	chromium- chromeos-release text/html	Chromium update for chromeos chromeos-release
1107815 - chromium - An open-source project to help move the web forward. - Monorail	Third Party Advisory crbug.com text/html	MISC crbug.com/1107815
[SECURITY] Fedora 33 Update: chromium-85.0.4183.83-1.fc33 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2020-6da740d38c
Chrome XRSystem::FocusedFrameChanged and FocusController::NotifyFocusChangedObservers Use-After-Free ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159611/Chrome-XRSystem-FocusedFrameChanged-and-FocusController-NotifyFocusChangedObservers-Use-After-Free.html
Debian -- Security Information -- DSA-4824-1 chromium	Third Party Advisory www.debian.org Deprecated Link text/html	DEBIAN DSA-4824
Qt WebEngine: Multiple vulnerabilities (GLSA 202101-30) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-202101-30

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

690527 Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (1110e286-dc08-11ea-beed-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	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
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
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:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

```
cpe:2.3:a:google:chrome:*.:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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