

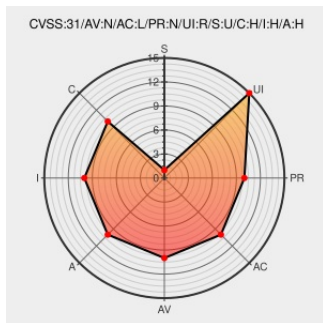


CVE-2020-6496

Published on: 06/03/2020 12:00:00 AM UTC

Last Modified on: 09/16/2021 01:44:00 PM UTC

CVE-2020-6496

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

Certain versions of [Macos](#) from [Apple](#) contain the following vulnerability:

Use after free in payments in Google Chrome on MacOS prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.

CVE-2020-6496 has been assigned by [chrome-cve-admin@google.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Google](#) - **Chrome** version < 83.0.4103.97

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: **6.8 - MEDIUM**

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

CVE References

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

Chrome Releases: Stable Channel Update for Desktop	Vendor Advisory chromereleases.googleblog.com text/html	 MISC chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop.html
Debian -- Security Information -- DSA-4714-1 chromium	www.debian.org Deprecated Link text/html	 DEBIAN DSA-4714
1085990 - chromium - An open-source project to help move the web forward. - Monorail	Permissions Required cbug.com text/html	 MISC cbug.com/1085990
[security-announce] openSUSE-SU-2020:0823-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:0823
[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	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	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
Operating System	Opensuse	Leap	15.1	All	All	All
cpe:2.3:o:apple:macos:-:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						

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:o:opensuse:leap:15.1:*.*.*.*.*.*.*.*

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:o:opensuse:leap:15.1:*.*.*.*.*.*.*.*

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:o:opensuse:leap:15.1:*.*.*.*.*.*.*.*.*

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:o:opensuse:leap:15.1:*.*.*.*.*.*.*.*.*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

Source	Title	Posted (UTC)
--------	-------	--------------

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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