



CVE-2020-15964

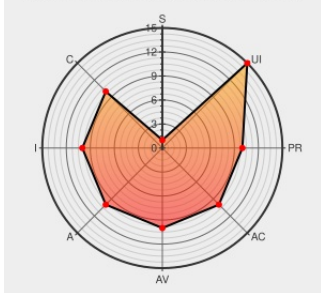
Published on: 09/21/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:17:00 AM UTC

CVE-2020-15964

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

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



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

Insufficient data validation in media in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-15964 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Google - Chrome** version < 85.0.4183.121

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
1121414 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Issue Tracking	MISC cbug.com/1121414

move the web forward: chromium	Fedora Tracking Vendor Advisory crlbug.com text/html	
[SECURITY] Fedora 33 Update: chromium-85.0.4183.121-1.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-2d994b986d
Chrome Releases: Stable Channel Update for Desktop	Release Notes Vendor Advisory chromereleases.googleblog.com text/html	 MISC chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop_21.html
Chromium, Google Chrome: Multiple vulnerabilities (GLSA 202009-13) — Gentoo security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-202009-13
[security-announce] openSUSE-SU-2020:1542-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:1542
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
[security-announce] openSUSE-SU-2020:1713-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:1713
[SECURITY] Fedora 32 Update: chromium-85.0.4183.121-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-214865ce21
[SECURITY] Fedora 31 Update: chromium-85.0.4183.121-1.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-aea86f913e
[security-announce] openSUSE-SU-2020:1550-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:1550
[security-announce] openSUSE-SU-2020:1527-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:1527

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

[690309](#) Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (e68d3db1-fd04-11ea-a67f-e09467587c17)

[750629](#) OpenSUSE Security Update for chromium (openSUSE-SU-2020:1527-1)

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	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	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:debian:debian_linux:10.0:*****:						
cpe:2.3:o:fedoraproject:fedora:31:*****:						
cpe:2.3:o:fedoraproject:fedora:32:*****:						
cpe:2.3:o:fedoraproject:fedora:33:*****:						
cpe:2.3:o:fedoraproject:fedora:31:*****:						
cpe:2.3:o:fedoraproject:fedora:32:*****:						

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

[← Previous ID](#)

[Next ID →](#)