



CVE-2020-6514

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-6514
State	PUBLIC
Assigner	chrome-cve-admin@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-22 17:15:00 UTC
Updated	2023-11-07 03:24:00 UTC
Description	Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipados	All	All	All	All
Operating System	Apple	Ipados	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Apple	Safari	All	All	All	All
Operating System	Apple	TvOS	All	All	All	All
Operating System	Apple	TvOS	All	All	All	All
Operating System	Apple	WatchOS	All	All	All	All
Operating System	Apple	WatchOS	All	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All

Operating System	Debian	Debian Linux	9.0	All	All	All
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
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
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

References

Reference	Source	Link
About the security content of watchOS 6.2.8 - Apple Support	CONFIRM	support.apple.com
[security-announce] openSUSE-SU-2020:1048-1: important: Security update	SUSE	lists.opensuse.org
[security-announce] openSUSE-SU-2020:1148-1: moderate: Security update f	SUSE	lists.opensuse.org
Chromium, Google Chrome: Multiple vulnerabilities (GLSA 202007-08) — Gentoo security	GENTOO	security.gentoo.org
[security-announce] openSUSE-SU-2020:1172-1: moderate: Security update f	SUSE	lists.opensuse.org
tvOS 13.4.8'in güvenlik içeriği hakkında - Apple Destek	CONFIRM	support.apple.com
Chrome Releases: Stable Channel Update for Desktop	MISC	chromereleases.googleusercontent.com
Debian -- Security Information -- DSA-4740-1 thunderbird	DEBIAN	www.debian.org
[security-announce] openSUSE-SU-2020:1189-1: important: Security update	SUSE	lists.opensuse.org
[security-announce] openSUSE-SU-2020:1205-1: important: Security update	SUSE	lists.opensuse.org
About the security content of Safari 13.1.2 - Apple Support	CONFIRM	support.apple.com
[SECURITY] Fedora 31 Update: chromium-84.0.4147.89-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 2297-1] firefox-esr security update	MLIST	lists.debian.org
1076703 - chromium - An open-source project to help move the web forward. - Monorail	MISC	crbug.com
WebRTC usrsctp Incorrect Call ≈ Packet Storm	MISC	packetstormsecurity.com

[security-announce] openSUSE-SU-2020:114/-1: important: Security update	SUSE	lists.opensuse.org
Mozilla Thunderbird: Multiple vulnerabilities (GLSA 202007-64) — Gentoo security	GENTOO	security.gentoo.org
About the security content of iOS 13.6 and iPadOS 13.6 - Apple Support	CONFIRM	support.apple.com
[SECURITY] Fedora 32 Update: chromium-84.0.4147.89-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Debian -- Security Information -- DSA-4824-1 chromium	DEBIAN	www.debian.org
Qt WebEngine: Multiple vulnerabilities (GLSA 202101-30) — Gentoo security	GENTOO	security.gentoo.org
USN-4443-1: Firefox vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
[SECURITY] [DLA 2310-1] thunderbird security update	MLIST	lists.debian.org
[security-announce] openSUSE-SU-2020:1155-1: important: Security update	SUSE	lists.opensuse.org
[security-announce] openSUSE-SU-2020:1179-1: important: Security update	SUSE	lists.opensuse.org
[SECURITY] Fedora 32 Update: chromium-84.0.4147.89-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[security-announce] openSUSE-SU-2020:1061-1: important: Security update	SUSE	lists.opensuse.org
[SECURITY] Fedora 31 Update: chromium-84.0.4147.89-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Debian -- Security Information -- DSA-4736-1 firefox-esr	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [296072](#) Oracle Solaris 11.4 Support Repository Update (SRU) 25.75.3 Missing (CPUJUL2020)
- [377050](#) Alibaba Cloud Linux Security Update for firefox (ALINUX2-SA-2020:0109)
- [500932](#) Alpine Linux Security Update for firefox-esr
- [500952](#) Alpine Linux Security Update for firefox
- [501075](#) Alpine Linux Security Update for mozjs68
- [503837](#) Alpine Linux Security Update for firefox
- [690466](#) Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (870d59b0-c6c4-11ea-8015-e09467587c17)

© CVE.report 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](#).

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