



CVE-2020-15999

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

Summary

CVE	CVE-2020-15999
State	PUBLIC
Assigner	chrome-cve-admin@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-03 03:15:00 UTC
Updated	2024-01-15 14:15:00 UTC
Description	Heap buffer overflow in FreeType in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit r

Risk And Classification

EPSS: 0.929310000 probability, percentile 0.997720000 (date 2026-04-01)

CISA KEV: Listed on 2021-11-03; due 2021-11-17; ransomware use Unknown

Problem Types: CWE-787

CISA Known Exploited Vulnerability

Vendor	Google
Product	Chrome FreeType
Name	Google Chrome FreeType Heap Buffer Overflow Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-15999

NVD Known Affected Configurations (CPE 2.3)

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	31	All	All	All
Application	Freetype	Freetype	All	All	All	All
Application	Freetype	Freetype2	All	All	All	All
Application	Freetype	Freetype2	All	All	All	All
Application	Google	Chrome	All	All	All	All

Application	Google	Chrome	All	All	All	All
Application	Opensuse	Backports Sle	15.0	sp2	All	All
Application	Opensuse	Backports Sle	15.0	sp2	All	All

References

Reference	Source	Link
Mozilla Thunderbird: Multiple vulnerabilities (GLSA 202012-04) — Gentoo security	GENTOO	security.gentoo.org
Chrome Releases: Stable Channel Update for Desktop	MISC	chromereleases.googleblo
[security-announce] openSUSE-SU-2020:1829-1: important: Security update	SUSE	lists.opensuse.org
[SECURITY] Fedora 31 Update: freetype-2.10.0-4.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Debian -- Security Information -- DSA-4824-1 chromium	DEBIAN	www.debian.org
Opera: Multiple Vulnerabilities (GLSA 202401-19) — Gentoo security		security.gentoo.org
[SECURITY] Fedora 31 Update: freetype-2.10.0-4.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Project Zero: CVE-2020-15999: FreeType Heap Buffer Overflow in Load_SBit_Png	MISC	googleprojectzero.blogspo
Full Disclosure: TCMalloc viewer/dumper - TCMalloc Inspector Tool	FULLDISC	seclists.org
1139963 - chromium - An open-source project to help move the web forward. - Monorail	MISC	crbug.com
Chromium, Google Chrome: Multiple vulnerabilities (GLSA 202011-12) — Gentoo security	GENTOO	security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296070](#) Oracle Solaris 11.4 Support Repository Update (SRU) 28.82.3 Missing (CPUOCT2020)

[354305](#) Amazon Linux Security Advisory for freetype : ALAS2022-2022-033

[354399](#) Amazon Linux Security Advisory for freetype : ALAS2022-2022-154

[355187](#) Amazon Linux Security Advisory for freetype : ALAS2023-2023-074

[376909](#) Alibaba Cloud Linux Security Update for freetype (ALINUX2-SA-2020:0175)

[500188](#) Alpine Linux Security Update for freetype

[500937](#) Alpine Linux Security Update for firefox-esr

[500957](#) Alpine Linux Security Update for firefox

[502376](#) Alpine Linux Security Update for thunderbird

503842 Alpine Linux Security Update for firefox
503929 Alpine Linux Security Update for freetype
504804 Alpine Linux Security Update for firefox-esr
505444 Alpine Linux Security Update for thunderbird
690387 Free Berkeley Software Distribution (FreeBSD) Security Update for freetype2 (458df97f-1440-11eb-aaec-e0d55e2a8bf9)
690393 Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (f4722927-1375-11eb-8711-3065ec8fd3ec)
710836 Gentoo Linux Opera Multiple Vulnerabilities (GLSA 202401-19)
750472 OpenSUSE Security Update for MozillaFirefox (openSUSE-SU-2020:2315-1)
750511 OpenSUSE Security Update for MozillaThunderbird (openSUSE-SU-2020:2187-1)
750538 OpenSUSE Security Update for MozillaThunderbird (openSUSE-SU-2020:2096-1)
750563 OpenSUSE Security Update for MozillaFirefox (openSUSE-SU-2020:2031-1)
750570 OpenSUSE Security Update for MozillaFirefox (openSUSE-SU-2020:2020-1)
750593 OpenSUSE Security Update for opera (openSUSE-SU-2020:1952-1)
750950 OpenSUSE Security Update for python-CairoSVG, python-Pillow (openSUSE-SU-2021:1134-1)
900615 Common Base Linux Mariner (CBL-Mariner) Security Update for freetype (8321)
901598 Common Base Linux Mariner (CBL-Mariner) Security Update for freetype (8324-1)
940232 AlmaLinux Security Update for freetype (ALSA-2020:4952)
960223 Rocky Linux Security Update for freetype (RLSA-2020:4952)
982958 Dotnet (nuget) Security Update for CefSharp.Wpf.HwndHost (GHSA-pv36-h7jh-qm62)

© [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](#) 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](#)