



# CVE-2020-28915

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-28915
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-18 08:15:00 UTC
<b>Updated</b>	2020-12-15 19:52:00 UTC
<b>Description</b>	A buffer over-read (at the framebuffer layer) in the fbcon code in the Linux kernel before 5.8.15 could be used by local attac

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

## References

Reference	Source	Link
KASAN: global-out-of-bounds Read in fbcon_get_font	MISC	<a href="https://syzkaller.appspot.com">syzkaller.appspot.com</a>
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.8.15	MISC	<a href="https://cdn.kernel.org">cdn.kernel.org</a>
Bug 1178886 – VUL-0: CVE-2020-28915: kernel-source: kernel buffer overflow read in font handling	MISC	<a href="https://bugzilla.suse.com">bugzilla.suse.com</a>
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

159962 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5316)

240528 Red Hat Update for kernel-rt (RHSA-2022:5344)
240534 Red Hat Update for kernel (RHSA-2022:5316)
353100 Amazon Linux Security Advisory for kernel : ALAC2012-2021-024
353101 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025
353102 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026
375284 EulerOS Security Update for kernel (EulerOS-SA-2021-1311)
390217 Oracle Managed Virtualization (VM) Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2021-0001)
390234 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0001)
670185 EulerOS Security Update for kernel (EulerOS-SA-2021-1684)
750376 OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
750488 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2260-1)
750518 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2161-1)
750568 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2034-1)
900040 CBL-Mariner Linux Security Update for kernel 5.4.91
903331 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3630)
906170 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3630-1)
940589 AlmaLinux Security Update for kernel-rt (ALSA-2022:5344)
940593 AlmaLinux Security Update for kernel (ALSA-2022:5316)
960258 Rocky Linux Security Update for kernel-rt (RLSA-2022:5344)
960418 Rocky Linux Security Update for kernel (RLSA-2022:5316)

© [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](#)**