



CVE-2020-14386

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

Summary

CVE	CVE-2020-14386
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-16 13:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	A flaw was found in the Linux kernel before 5.9-rc4. Memory corruption can be exploited to gain root privileges from unprivi

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc1	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc2	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc3	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc1	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc2	All	All
Operating System	Linux	Linux Kernel	5.9.0	rc3	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source
[security-announce] openSUSE-SU-2020:1655-1: important: Security update	SUSE
[SECURITY] [DLA 2420-2] linux regression update	MLIST
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC

oss-security - Re: Containers-optimized OS (COS) membership in the linux-distros list	MLIST
oss-security - Re: Containers-optimized OS (COS) membership in the linux-distros list	MLIST
[SECURITY] [DLA 2385-1] linux-4.19 security update	MLIST
Kernel Live Patch Security Notice LSN-0072-1 ≈ Packet Storm	MISC
oss-sec: CVE-2020-14386: Linux kernel: af_packet.c vulnerability	MISC
1875699 – (CVE-2020-14386) CVE-2020-14386 kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege	CONFIF
oss-security - Containers-optimized OS (COS) membership in the linux-distros list	MLIST
[SECURITY] Fedora 33 Update: kernel-5.8.7-300.fc33 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 33 Update: kernel-5.8.7-300.fc33 - package-announce - Fedora Mailing-Lists	FEDOR
[SECURITY] [DLA 2420-1] linux security update	MLIST
CVE Program record	CVE.OP
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [352341](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-027
- [352342](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-026
- [352343](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-025
- [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
- [353136](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-015
- [376992](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0115)
- [6140338](#) AWS Bottlerocket Security Update for kernel (GHSA-53mq-2mw5-rjcr)
- [750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
- [900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [902891](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3470)
- [905955](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3470-1)

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