



CVE-2020-14385

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

Summary

CVE	CVE-2020-14385
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-15 22:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	A flaw was found in the Linux kernel before 5.9-rc4. A failure of the file system metadata validator in XFS can cause an inc

Risk And Classification

Problem Types: CWE-131

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.9.0	-	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	-	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

References

Reference

[USN-4576-1: Linux kernel vulnerabilities](#) | [Ubuntu security notices](#) | [Ubuntu](#)

1874800 – (CVE-2020-14385) CVE-2020-14385 kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended :

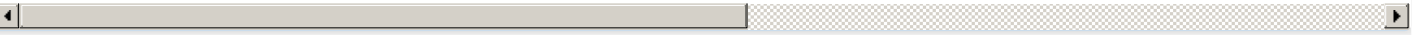
[SECURITY] [DLA 2385-1] linux-4.19 security update

kernel/git/torvalds/linux.git - Linux kernel source tree

[security-announce] openSUSE-SU-2020:1586-1: important: Security update

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[353135](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-016

[6140075](#) AWS Bottlerocket Security Update for kernel (GHSA-wj7m-fx22-c4cf)

[750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)

[900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91

[903225](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3461)

[906121](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3461-1)

© [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](#)