



CVE-2022-0480

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

Summary

CVE	CVE-2022-0480
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-29 15:15:00 UTC
Updated	2023-03-03 18:49:00 UTC
Description	A flaw was found in the filelock_init in fs/locks.c function in the Linux kernel. This issue can lead to host memory exhaustion

Risk And Classification

Problem Types: CWE-770

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
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source
CVE-2022-0480 Ubuntu	MI
[patch 101/212] memcg: enable accounting for file lock caches - Andrew Morton	MI
kernel/git/torvalds/linux.git - Linux kernel source tree	MI
[patch 101/212] memcg: enable accounting for file lock caches - Andrew Morton	MI
Host Memory Exhaustion Attack from Inside Kata Containers · Issue #3373 · kata-containers/kata-containers · GitHub	MI
2049700 – (CVE-2022-0480) CVE-2022-0480 kernel: memcg does not limit the number of POSIX file locks allowing memory exhaustion	MI
Red Hat Customer Portal - Access to 24x7 support and knowledge	MI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[183102](#) Debian Security Update for linux (CVE-2022-0480)

[243050](#) Red Hat Update for kernel (RHSA-2024:1250)

[243059](#) Red Hat Update for kernel-rt (RHSA-2024:1303)

[243060](#) Red Hat Update for kernel security (RHSA-2024:1304)

[243062](#) Red Hat Update for kernel-rt (RHSA-2024:1306)

[905672](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13752)

© [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](#)