



CVE-2021-4023

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

Summary

CVE	CVE-2021-4023
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-10 17:44:00 UTC
Updated	2022-03-15 17:10:00 UTC
Description	A flaw was found in the io-workqueue implementation in the Linux kernel versions prior to 5.15-rc1. The kernel can panic w

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference
2026484 – (CVE-2021-4023) CVE-2021-4023 kernel: Improper IO-uring request cancellation operation allows local users to cause a crash
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

183463 Debian Security Update for linux (CVE-2021-4023)
900749 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8943)
901314 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8943-1)
906102 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8943-2)

© [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](#)