

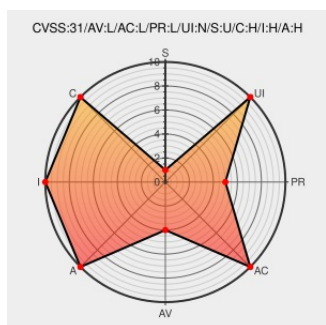


CVE-2022-1976

Published on: Not Yet Published

Last Modified on: 02/14/2023 01:15:00 PM UTC

CVE-2022-1976

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

A flaw was found in the Linux kernel's implementation of IO-URING. This flaw allows an attacker with local executable permission to create a string of requests that can cause a use-after-free flaw within the kernel. This issue leads to memory corruption and possible privilege escalation.

CVE-2022-1976 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	MISC git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=9cae36a094e7e9d6e5fe8b6dcd4642138b3eb0c7
2092549 – (CVE-2022-1976) CVE-2022-1976 kernel: incorrect in-flight accounting in io_uring leads to use-after-free	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=2092549
August 2022 Linux Kernel 5.18 Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20230214-0005/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

Related QID Numbers

[183729](#) Debian Security Update for linux (CVE-2022-1976)

[903717](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10813)

[903854](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10821)

[904102](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10813-1)

[904252](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10821-1)

[905920](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10813-2)

[906496](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10821-2)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:linux:linux_kernel:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-1976 : A flaw was found in the #Linux #kernel's implementation of IO-URING. This flaw allows an attacker w... twitter.com/i/web/status/1...	2022-08-31 16:09:59

[← Previous ID](#)[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)