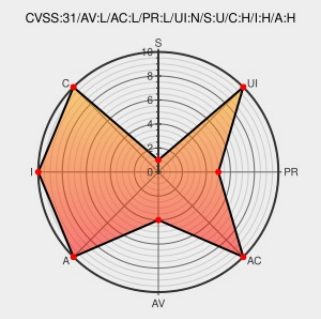
CVE-2022-1976

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/

comment@cve.report.

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→