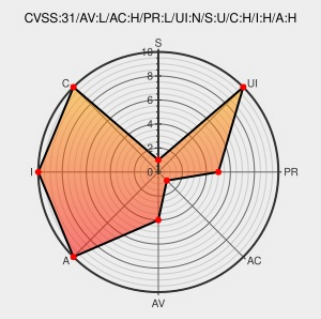
CVE-2022-2961

Published on: Not Yet Published

Last Modified on: 06/28/2023 08:34:00 PM UTC

CVE-2022-2961

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

A use-after-free flaw was found in the Linux kernel's PLP Rose functionality in the way a user triggers a race condition by calling bind while simultaneously triggering the rose_bind() function. This flaw allows a local user to crash or potentially escalate their privileges on the system.

CVE-2022-2961 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7 - HIGH

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

CVE References

Description	Tags	Link
August 2022 Linux Kernel 5.19 Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20230214-0004/
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2022-2961

Related QID Numbers

903759 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10778)

903838 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10761)

Exploit/POC from Github

A use-after-free flaw was found in the Linux kernel's PLP Rose functionality in the way a user triggers a race condit…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	6.0	rc1	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.0:rc1:*:*:*:*:*:*:

cpe:2.3:h:netapp:h300s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h300s_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h410c:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h410c_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h410s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h410s_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h500s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h500s_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h700s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h700s_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-2961 : A use-after-free flaw was found in the #Linux #kernel's PLP Rose functionality in the way a user tr… twitter.com/i/web/status/1…	2022-08-29 15:15:37
@LinInfoSec	Bind - CVE-2022-2961: access.redhat.com/security/cve/C…	2022-08-29 17:01:12
/r/netcve	CVE-2022-2961	2022-08-29 16:38:48
/r/KomodoCyberConsulting	CVE-2022-2961: Linux Kernel Privilege Escalation Vulnerability	2022-08-30 12:14:07

← Previous ID

Next ID→