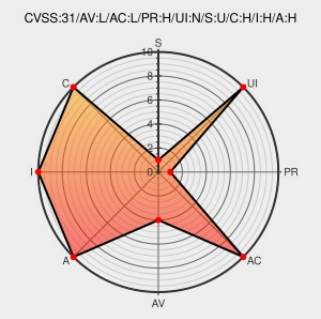
CVE-2022-42464

Published on: Not Yet Published

Last Modified on: 10/18/2022 07:39:00 PM UTC

CVE-2022-42464

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



Certain versions of Openharmony from Openharmony contain the following vulnerability:

OpenHarmony-v3.1.2 and prior versions, 3.0.6 and prior versions have a Kernel memory pool override vulnerability in /dev/mmz_userdev device driver. The impact depends on the privileges of the attacker. The unprivileged process run on the device could disclose sensitive information including kernel pointer, which could be used in further attacks. The processes with system user UID run on the device would be able to mmap memory pools used by kernel and override them which could be used to gain kernel code execution on the device, gain root privileges, or cause device reboot.

CVE-2022-42464 has been assigned by scy@openharmony.io to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **OpenHarmony** - **OpenHarmony** version **<= 3.1.2**

Affected Vendor/Software: **OpenHarmony** - **OpenHarmony** version **<= 3.0.6**

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
en/security-disclosure/2022/2022-10.md · OpenHarmony/security - Gitee.com	gitee.com text/html	MISC gitee.com/openharmony/security/blob/master/en/security-disclosure/2022/2022-10.md

CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openharmony	Openharmony	All	All	All	All
Application	Openharmony	Openharmony	All	All	All	All

cpe:2.3:a:openharmony:openharmony:*:*:*:*:*:*:*:*:

cpe:2.3:a:openharmony:openharmony:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-42464 : OpenHarmony-v3.1.2 and prior versions, 3.0.6 and prior versions have a Kernel memory pool override… twitter.com/i/web/status/1…	2022-10-14 15:11:36
/r/netcve	CVE-2022-42464	2022-10-14 15:39:19

← Previous ID

Next ID→