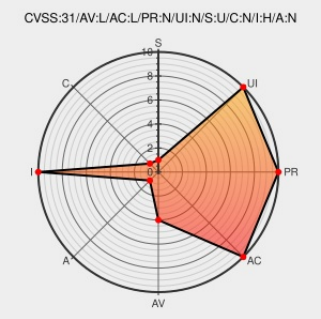
CVE-2022-38081

Published on: Not Yet Published

Last Modified on: 09/14/2022 09:18:00 PM UTC

CVE-2022-38081

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 have a permission bypass vulnerability. LAN attackers can bypass the distributed permission control.To take advantage of this weakness, attackers need another vulnerability to obtain system.

CVE-2022-38081 has been assigned by scy@openharmony.io to track the vulnerability - currently rated as MEDIUM severity.

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

CVSS3 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
en/security-disclosure/2022/2022-09.md · OpenHarmony/security - Gitee.com	gitee.com text/html	MISC gitee.com/openharmony/security/blob/master/en/security-disclosure/2022/2022-09.md

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-38081 : OpenHarmony-v3.1.2 and prior versions have a permission bypass vulnerability. LAN attackers can by… twitter.com/i/web/status/1…	2022-09-09 15:28:20
/r/netcve	CVE-2022-38081	2022-09-09 16:38:43

← Previous ID

Next ID→