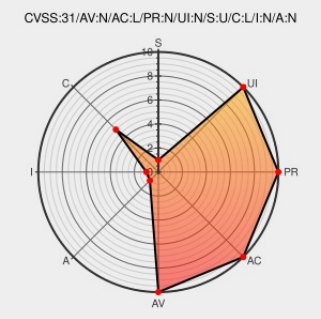
CVE-2020-9846

Published on: Not Yet Published

Last Modified on: 03/07/2023 07:58:00 PM UTC

CVE-2020-9846

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



Certain versions of Macos from Apple contain the following vulnerability:

A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.0.1. A malicious application may be able to access local users' Apple IDs.

CVE-2020-9846 has been assigned by product-security@apple.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Apple** - **macOS** version **< 12.0**

CVSS3 Score: 5.3 - MEDIUM

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

CVE References

Description	Tags	Link
About the security content of macOS Monterey 12.0.1 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT212869

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	All	All	All	All

cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→