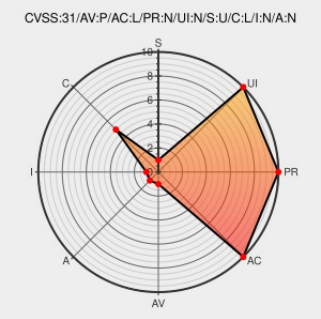
CVE-2023-32417

Published on: Not Yet Published

Last Modified on: 09/06/2023 08:15:00 AM UTC

CVE-2023-32417

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



Certain versions of Watchos from Apple contain the following vulnerability:

This issue was addressed by restricting options offered on a locked device. This issue is fixed in watchOS 9.5. An attacker with physical access to a locked Apple Watch may be able to view user photos or contacts via accessibility features.

CVE-2023-32417 has been assigned by product-security@apple.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **Apple** - **watchOS** version **< 9.5**

CVSS3 Score: 2.4 - LOW

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	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 Ventura 13.4 - Apple Support	support.apple.com text/html	MISC support.apple.com/kb/HT213758
About the security content of watchOS 9.5 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT213764

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution PATCH: NOW	2023-05-19 12:09:54

← Previous ID

Next ID→