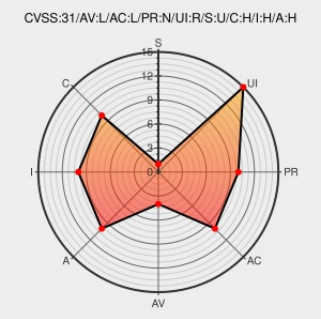
CVE-2020-9992

Published on: 10/16/2020 12:00:00 AM UTC

Last Modified on: 01/09/2023 04:41:00 PM UTC

CVE-2020-9992

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



Certain versions of Ipados from Apple contain the following vulnerability:

This issue was addressed by encrypting communications over the network to devices running iOS 14, iPadOS 14, tvOS 14, and watchOS 7. This issue is fixed in iOS 14.0 and iPadOS 14.0, Xcode 12.0. An attacker in a privileged network position may be able to execute arbitrary code on a paired device during a debug session over the network.

CVE-2020-9992 has been assigned by product-security@apple.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Apple** - **iOS** version **< iOS 14.0 and iPadOS 14.0**

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

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
About the security content of iOS 14.0 and iPadOS 14.0 - Apple Support	Release Notes Vendor Advisory support.apple.com text/html	MISC support.apple.com/HT211850
About the security content of Xcode 12.0 - Apple Support	Release Notes Vendor Advisory support.apple.com text/html	MISC support.apple.com/HT211848
Full Disclosure: APPLE-SA-2020-11-13-3 Additional information for APPLE-SA-2020-09-16-1 iOS 14.0 and iPadOS 14.0	seclists.org text/html	FULLDISC 20201115 APPLE-SA-2020-11-13-3 Additional information for APPLE-SA-2020-09-16-1 iOS 14.0 and iPadOS 14.0

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2020-9992 - A design flaw in MobileDevice.framework/Xcode and iOS/iPadOS/tvOS Development Tools allows an attacke…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipados	All	All	All	All
Operating System	Apple	Ipad Os	All	All	All	All
Operating System	Apple	Ipad Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Application	Apple	Xcode	All	All	All	All
Application	Apple	Xcode	All	All	All	All

cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:ipad_os:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:ipad_os:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:

cpe:2.3:a:apple:xcode:*:*:*:*:*:*:*:*:

cpe:2.3:a:apple:xcode:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ??? | This issue was addressed by encrypting c... | CVE-2020-9992 | Link for more: alerts.remotelyrmm.com/CVE-2020-9992	2022-05-24 15:28:19

← Previous ID

Next ID→