

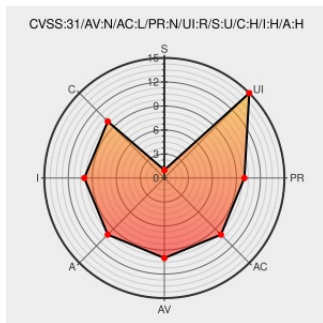


CVE-2020-3843

Published on: 02/27/2020 12:00:00 AM UTC

Last Modified on: 05/31/2022 03:54:00 PM UTC

CVE-2020-3843

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Iphone Os](#) from [Apple](#) contain the following vulnerability:

A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4.7, watchOS 5.3.7. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.

CVE-2020-3843 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Apple** - **iOS-1** version < **iOS 12.4.7**

Affected Vendor/Software: **Apple** - **watchOS-1** version < **watchOS 5.3.7**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	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
Apple iOS 12.4.7, watchOS 5.3.7, tvOS 12.4.7, macOS 10.14.6, and macOS 10.15.2	Apple, iOS, watchOS, tvOS, macOS	https://support.apple.com/kb/HT204400

About the security content of iOS 12.4.7 - Apple Support

support.apple.com
text/html

MISC support.apple.com/H1211169

iOS / macOS Radio Proximity Kernel Memory Corruption ≈ Packet Storm

packetstormsecurity.com
text/html

MISC packetstormsecurity.com/files/162119/iOS-macOS-Radio-Proximity-Kernel-Memory-Corruption.html

About the security content of watchOS 5.3.7 - Apple Support

support.apple.com
text/html

MISC support.apple.com/HT211176

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, 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
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
cpe:2.3:o:apple:iphone_os:*****:.*						
cpe:2.3:o:apple:mac_os_x:*****:.*						
cpe:2.3:o:apple:mac_os_x:*****:.*						
cpe:2.3:o:apple:watchos:*****:.*						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ??? A memory corruption issue was addressed ... CVE-2020-3843 Link for more: alerts.remotelyrmm.com/CVE-2020-3843	2022-05-31 17:28:56
 @4ng3n01r3	#CyberSecurity #Security #CERT #CVE #Nist #Analysed #breach #vulnerability : CVE-2020-3843 (iphone_os, watchos)	2022-05-31 18:07:30

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)