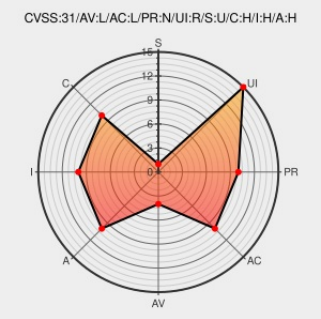
CVE-2020-27930

Published on: 12/08/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:29 PM UTC

CVE-2020-27930

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



Certain versions of Ipados from Apple contain the following vulnerability:

A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. Processing a maliciously crafted font may lead to arbitrary code execution.

CVE-2020-27930 has been assigned by product-security@apple.com to track the vulnerability - currently rated as HIGH severity.

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: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
About the security content of watchOS 7.1 - Apple Support	Vendor Advisory	MISC support.apple.com/en-us/HT211928

About the security content of watchOS 7.1 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/en-us/HT211928
About the security content of iOS 14.2 and iPadOS 14.2 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/en-us/HT211929
Full Disclosure: APPLE-SA-2020-12-14-4 Additional information for APPLE-SA-2020-11-13-1 macOS Big Sur 11.0.1	Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20201215 APPLE-SA-2020-12-14-4 Additional information for APPLE-SA-2020-11-13-1 macOS Big Sur 11.0.1
Apple Safari Remote Code Execution ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/161294/Apple-Safari-Remote-Code-Execution.html
About the security content of macOS Big Sur 11.0.1 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/en-us/HT211931
About the security content of watchOS 5.3.9 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/en-us/HT211945
About the security content of watchOS 6.2.9 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/en-us/HT211944
About the security content of Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/en-us/HT211946
About the security content of macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/en-us/HT211947
About the security content of iOS 12.4.9 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/en-us/HT211940

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Apple Safari Remote Code Execution

Known Affected Configurations (CPE V2.3)

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

Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Macos	All	All	All	All
Operating System	Apple	Macos	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
Operating System	Apple	Watchos	All	All	All	All

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

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

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

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

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

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

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
𝕏 @ipssignatures	It's new to me that Astaro has a protection/signature/rule for the vulnerability CVE-2020-27930.… twitter.com/i/web/status/1…	2021-11-11 06:02:01
𝕏 @ipssignatures	It is the first time for me to know a protection/signature/rule for the vulnerability CVE-2020-27930. #Swjtb2pltmpuee	2021-11-11 06:02:01

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report