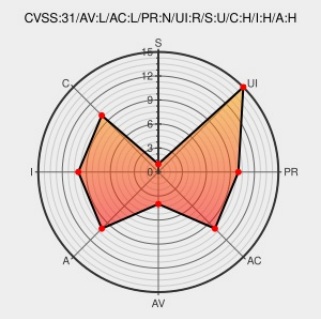
CVE-2020-27904

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

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

CVE-2020-27904

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



Certain versions of Macos from Apple contain the following vulnerability:

A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1. An application may be able to execute arbitrary code with kernel privileges.

CVE-2020-27904 has been assigned by product-security@apple.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Apple** - **macOS** version **< 11.0**

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
Full Disclosure: APPLE-SA-2021-02-01-1 macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave	Mailing List Third Party Advisory seclists.org	FULLDISC 20210201 APPLE-SA-2021-02-01-1 macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave

	text/html	
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
About the security content of macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT212147
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

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	Macos	All	All	All	All
Operating System	Apple	Macos	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@matteyeux	Demo exploit code for CVE-2020-27904, a tfp0 bug. github.com/pattern-f/xatt…	2021-05-07 07:07:03
@iFenixx	Demo exploit code for CVE-2020-27904, a tfp0 bug. github.com/pattern-f/xatt…	2021-05-07 07:23:18
@JBsite12	Demo exploit code CVE-2020-27904 github: github.com/pattern-f/xatt… #jailbreak #exploit	2021-05-07 07:43:07
@oss_clang	xattr-oob-swap - Demo exploit code for CVE-2020-27904, a tfp0 bug. github.com/pattern-f/xatt…	2021-05-07 08:01:30
@ipssignatures	I know no IPS that has a protection/signature/rule for the vulnerability CVE-2020-27904. The vuln was published 149… twitter.com/i/web/status/1…	2021-05-07 09:04:02
@ipssignatures	The vuln CVE-2020-27904 has a tweet created 0 days ago and retweeted 8 times. twitter.com/matteyeux/stat… #Sb2jxxtr6auezc	2021-05-07 09:04:02

@ipssignatures	The vuln CVE-2020-27904 has a tweet created 0 days ago and retweeted 18 times. twitter.com/matteyeux/stat… #pow1rtrtwwcve	2021-05-07 11:06:00
@ipssignatures	The vuln CVE-2020-27904 has a tweet created 0 days ago and retweeted 10 times. twitter.com/iFenixx/status… #pow1rtrtwwcve	2021-05-07 11:06:00

← Previous ID

Next ID→

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