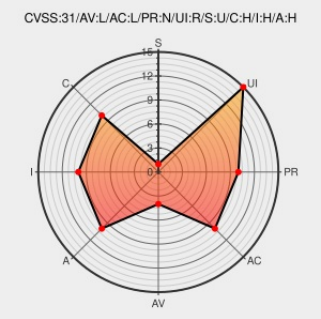
CVE-2019-8561

Published on: 12/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:55 PM UTC

CVE-2019-8561

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



Certain versions of Mac Os X from Apple contain the following vulnerability:

A logic issue was addressed with improved validation. This issue is fixed in macOS Mojave 10.14.4. A malicious application may be able to elevate privileges.

CVE-2019-8561 has been assigned by product-security@apple.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Apple** - **macOS** version **< macOS Mojave 10.14.4**

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 macOS Mojave 10.14.4, Security Update 2019-002 High Sierra, Security Update 2019-002 Sierra - Apple Support	Vendor Advisory, support.apple.com, text/html	MISC support.apple.com/HT209600

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

Exploit/POC from Github

Proof of concept exploit for CVE-2019-8561 discovered by @jbradley89

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@0xmachos	Writeup and Poof of Concept exploit for @jbradley89's CVE-2019-8561, exploitable up to macOS 10.14.3 to get r00t an… twitter.com/i/web/status/1…	2021-04-30 13:52:09
@ipssignatures	The vuln CVE-2019-8561 has a tweet created 0 days ago and retweeted 11 times. twitter.com/0xmachos/statu… #pow1rtrtwwcve	2021-05-01 03:06:00
@0xmachos	Closely followed by @jbradley89's CVE-2019-8561 youtube.com/watch?v=5nOxzn…	2021-07-22 13:07:00
@ksg93rd	#Threat_Research 1. A Hard-to-Banish PackageKit Framework Vulnerability in macOS (CVE-2019-8561)… twitter.com/i/web/status/1…	2022-11-12 16:26:10
@PentestingN	A Hard-to-Banish PackageKit Framework Vulnerability in macOS (CVE-2019-8561) trendmicro.com/en_us/research… Google Pixel… twitter.com/i/web/status/1…	2022-11-12 17:13:49

← Previous ID

Next ID→

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