



CVE-2019-8852

Published on: 10/27/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-8852

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

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

A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.2, Security Update 2019-002 Mojave, and Security Update 2019-007 High Sierra. An application may be able to execute arbitrary code with kernel privileges.

CVE-2019-8852 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Apple** - **macOS** version < 10.15

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 macOS Catalina 10.15.2, Security Update 2019-002 Mojave,	Release Notes	MISC

