About the security content of Security Update 2021-003 Mojave

This document describes the security content of Security Update 2021-003 Mojave.

About Apple security updates

For our customers' protection, Apple doesn't disclose, discuss, or confirm security issues until an investigation has occurred and patches or releases are available. Recent releases are listed on the Apple security updates page.

Apple security documents reference vulnerabilities by CVE-ID when possible.

For more information about security, see the Apple Product Security page.

Security Update 2021-003 Mojave

Released April 26, 2021

APFS

Available for: macOS Mojave

Impact: A local user may be able to read arbitrary files

Description: The issue was addressed with improved permissions logic.

CVE-2021-1797: Thomas Tempelmann

Audio

Available for: macOS Mojave

Impact: An application may be able to read restricted memory

Description: A memory corruption issue was addressed with improved validation.

CVE-2021-1808: JunDong Xie of Ant Security Light-Year Lab

CFNetwork

Available for: macOS Mojave

Impact: Processing maliciously crafted web content may disclose sensitive user information

Description: A memory initialization issue was addressed with improved memory handling.

CVE-2021-1857: an anonymous researcher

CoreAudio

Available for: macOS Mojave

Impact: A malicious application may be able to read restricted memory

Description: A memory corruption issue was addressed with improved validation.

CVE-2021-1809: JunDong Xie of Ant Security Light-Year Lab

CoreGraphics

Available for: macOS Mojave

Impact: Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution

Description: A memory corruption issue was addressed with improved validation.

CVE-2021-1847: Xuwei Liu of Purdue University

CoreText

Available for: macOS Mojave

Impact: Processing a maliciously crafted font may result in the disclosure of process memory

Description: A logic issue was addressed with improved state management.

CVE-2021-1811: Xingwei Lin of Ant Security Light-Year Lab

curl

Available for: macOS Catalina

Impact: A malicious server may be able to disclose active services

Description: This issue was addressed with improved checks.

CVE-2020-8284: Marian Rehak

Entry added May 6, 2021

curl

Available for: macOS Mojave

Impact: A remote attacker may be able to cause a denial of service

Description: A buffer overflow was addressed with improved input validation.

CVE-2020-8285: xnynx

curl

Available for: macOS Mojave

Impact: An attacker may provide a fraudulent OCSP response that would appear valid

Description: This issue was addressed with improved checks.

CVE-2020-8286: an anonymous researcher

DiskArbitration

Available for: macOS Mojave

Impact: A malicious application may be able to modify protected parts of the file system

Description: A permissions issue existed in DiskArbitration. This was addressed with additional ownership checks.

CVE-2021-1784: Csaba Fitzl (@theevilbit) of Offensive Security, an anonymous researcher, and Mikko Kenttälä (@Turmio_) of SensorFu

FontParser

Available for: macOS Mojave

Impact: Processing a maliciously crafted font file may lead to arbitrary code execution

Description: An out-of-bounds read was addressed with improved input validation.

CVE-2021-1881: Hou JingYi (@hjy79425575) of Qihoo 360, an anonymous researcher, Xingwei Lin of Ant Security Light-Year Lab, and Mickey Jin of Trend Micro

FontParser

Available for: macOS Mojave

Impact: Processing a maliciously crafted font file may lead to arbitrary code execution

Description: A logic issue was addressed with improved state management.

CVE-2020-27942: an anonymous researcher

Foundation

Available for: macOS Mojave

Impact: A malicious application may be able to gain root privileges

Description: A validation issue was addressed with improved logic.

CVE-2021-1813: Cees Elzinga

ImageIO

Available for: macOS Mojave

Impact: Processing a maliciously crafted image may lead to arbitrary code execution

Description: This issue was addressed with improved checks.

CVE-2021-1843: Ye Zhang of Baidu Security

Intel Graphics Driver

Available for: macOS Mojave

Impact: An application may be able to execute arbitrary code with kernel privileges

Description: An out-of-bounds write was addressed with improved input validation.

CVE-2021-1805: ABC Research s.r.o. working with Trend Micro Zero Day Initiative

Intel Graphics Driver

Available for: macOS Mojave

Impact: An application may be able to execute arbitrary code with kernel privileges

Description: A race condition was addressed with additional validation.

CVE-2021-1806: ABC Research s.r.o. working with Trend Micro Zero Day Initiative

Intel Graphics Driver

Available for: macOS Mojave

Impact: A malicious application may be able to execute arbitrary code with kernel privileges

Description: An out-of-bounds write issue was addressed with improved bounds checking.

CVE-2021-1834: ABC Research s.r.o. working with Trend Micro Zero Day Initiative

Kernel

Available for: macOS Mojave

Impact: A malicious application may be able to disclose kernel memory

Description: A memory initialization issue was addressed with improved memory handling.

CVE-2021-1860: @0xalsr

Kernel

Available for: macOS Mojave

Impact: An application may be able to execute arbitrary code with kernel privileges

Description: A logic issue was addressed with improved state management.

CVE-2021-1851: @0xalsr

Kernel

Available for: macOS Mojave

Impact: A local attacker may be able to elevate their privileges

Description: A memory corruption issue was addressed with improved validation.

CVE-2021-1840: Zuozhi Fan (@pattern_F_) of Ant Group Tianqiong Security Lab

libxpc

Available for: macOS Mojave

Impact: A malicious application may be able to gain root privileges

Description: A race condition was addressed with additional validation.

CVE-2021-30652: James Hutchins

libxslt

Available for: macOS Mojave

Impact: Processing a maliciously crafted file may lead to heap corruption

Description: A double free issue was addressed with improved memory management.

CVE-2021-1875: Found by OSS-Fuzz

NSRemoteView

Available for: macOS Mojave

Impact: Processing maliciously crafted web content may lead to arbitrary code execution

Description: A use after free issue was addressed with improved memory management.

CVE-2021-1876: Matthew Denton of Google Chrome

Preferences

Available for: macOS Mojave

Impact: A local user may be able to modify protected parts of the file system

Description: A parsing issue in the handling of directory paths was addressed with improved path validation.

CVE-2021-1739: Zhipeng Huo (@R3dF09) and Yuebin Sun (@yuebinsun2020) of Tencent Security Xuanwu Lab (xlab.tencent.com)

smbx

Available for: macOS Mojave

Impact: An attacker in a privileged network position may be able to leak sensitive user information

Description: An integer overflow was addressed with improved input validation.

CVE-2021-1878: Aleksandar Nikolic of Cisco Talos (talosintelligence.com)

Tailspin

Available for: macOS Mojave

Impact: A local attacker may be able to elevate their privileges

Description: A logic issue was addressed with improved state management.

CVE-2021-1868: Tim Michaud of Zoom Communications

tcpdump

Available for: macOS Mojave

Impact: A remote attacker may be able to cause a denial of service

Description: This issue was addressed with improved checks.

CVE-2020-8037: an anonymous researcher

Time Machine

Available for: macOS Mojave

Impact: A local attacker may be able to elevate their privileges

Description: The issue was addressed with improved permissions logic.

CVE-2021-1839: Tim Michaud(@TimGMichaud) of Zoom Video Communications and Gary Nield of ECSC Group plc

Wi-Fi

Available for: macOS Mojave

Impact: An application may be able to cause unexpected system termination or write kernel memory

Description: A memory corruption issue was addressed with improved validation.

CVE-2021-1828: Zuozhi Fan (@pattern_F_) of Ant Group Tianqiong Security Lab

wifivelocityd

Available for: macOS Mojave

Impact: An application may be able to execute arbitrary code with system privileges

Description: The issue was addressed with improved permissions logic.

CVE-2020-3838: Dayton Pidhirney (@_watbulb)

WindowServer

Available for: macOS Mojave

Impact: A malicious application may be able to unexpectedly leak a user's credentials from secure text fields

Description: An API issue in Accessibility TCC permissions was addressed with improved state management.

CVE-2021-1873: an anonymous researcher

Additional recognition

CoreCrypto

We would like to acknowledge Andy Russon of Orange Group for their assistance.

Entry added May 6, 2021

Intel Graphics Driver

We would like to acknowledge Jack Dates of RET2 Systems, Inc. for their assistance.

Entry added May 6, 2021

Kernel

We would like to acknowledge GRIMM, Keyu Man, Zhiyun Qian, Zhongjie Wang, Xiaofeng Zheng, Youjun Huang, Haixin Duan, and an anonymous researcher for their assistance.

Entry added May 6, 2021

Mail

We would like to acknowledge Petter Flink, SecOps of Bonnier News for their assistance.

Entry added May 6, 2021

Safari

We would like to acknowledge an anonymous researcher for their assistance.

Entry added May 6, 2021

Security

We would like to acknowledge Xingwei Lin of Ant Security Light-Year Lab and john (@nyan_satan) for their assistance.

Entry added May 6, 2021

Published Date: November 02, 2023