APPLE-SA-2021-04-26-3 Security Update 2021-002 Catalina

From: Apple Product Security via Fulldisclosure <fulldisclosure () seclists org>
Date: Mon, 26 Apr 2021 15:51:38 -0700

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

APPLE-SA-2021-04-26-3 Security Update 2021-002 Catalina

Security Update 2021-002 Catalina addresses the following issues.
Information about the security content is also available at
https://support.apple.com/HT212326.

APFS
Available for: macOS Catalina
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

Archive Utility
Available for: macOS Catalina
Impact: A malicious application may bypass Gatekeeper checks
Description: A logic issue was addressed with improved state
management.
CVE-2021-1810: an anonymous researcher

Audio
Available for: macOS Catalina
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 Catalina
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 Catalina
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 Catalina
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 Catalina
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 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 Catalina
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 Catalina
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: Mikko Kenttälä (@Turmio_) of SensorFu, Csaba Fitzl (@theevilbit) of Offensive Security, and an anonymous researcher

FontParser
Available for: macOS Catalina
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 Catalina
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 Catalina
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

Foundation
Available for: macOS Catalina
Impact: An application may be able to gain elevated privileges
Description: A memory corruption issue was addressed with improved
validation.
CVE-2021-1882: Gabe Kirkpatrick (@gabe_k)

ImageIO
Available for: macOS Catalina
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 Catalina
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 Catalina
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 Catalina
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 Catalina
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 Catalina
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 Catalina
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

Login Window
Available for: macOS Catalina
Impact: A malicious application with root privileges may be able to

```
access private information
Description: This issue was addressed with improved entitlements.
CVE-2021-1824: Wojciech Reguła (@_r3ggi) of SecuRing

NSRemoteView
Available for: macOS Catalina
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 Catalina
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)
CVE-2021-1740: Zhipeng Huo (@R3dF09) and Yuebin Sun (@yuebinsun2020)
of Tencent Security Xuanwu Lab (xlab.tencent.com)

smbx
Available for: macOS Catalina
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 Catalina
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 Catalina
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 Catalina
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 Catalina
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 Catalina
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)

Windows Server
Available for: macOS Catalina
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

Installation note:

This update may be obtained from the Mac App Store or
Apple's Software Downloads web site:
https://support.apple.com/downloads/

Information will also be posted to the Apple Security Updates
web site: https://support.apple.com/kb/HT201222

This message is signed with Apple's Product Security PGP key,
and details are available at:
https://www.apple.com/support/security/pgp/

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEEbURczHs1TP07VIfuZcsbuWJ6jjAFAmCHO1YACgkQZcsbuWJ6
jjBNDA//cITX6Bzw+4rkTd58ZQ+2P60B30bvuMWuNmXDEyIHZz0ZMDX7Wymm9SBC
GLQ9mh9XY10/11NjdAiHZIs8BTs18CcOpjODbRTuF7d/plL6eUcsSLVbkC9hoyJF
IOAEawLoqye7f+hlsCbC00NzLlAtsR5PjkqwCTGjGBw8G8qPbLFvh72Qwagr/G05
zeEg3fRM+lecFHUZzXVkdW2WiQ6aO2ejKkhdhSCATnj+xZF1wEz/Wjb3oLQ3qOvq
i8lQg7Vcr64uF0HGCKPBmbINc7yM/ChZjs5oEyxdMc1/rxvU30nSvEc17LsVMIvM
ZJxnjhBjcTi36gL8pM8Lfh57+AG0L/EwVe6onjC7yBneEbfk5dUYuglcAB2uJwgj
V47KS0+5X9bwi33JmI/OpaaVRVCqJBO+iiZQnuQFAFFcC/F2fu6g8uKg8Vo/kg/I
d4ypBrAsybJKZvMUVKBAWb9tS0JlVKpYurl89n9F2N47BkotP4AwDsmTTFZguiG+
sfRL+uAB2xy46VvLTNx71HeFTltc7wmlZOORx7MJ4bcYI/ibJbOq612Q7GyiADeP
cKKpi4snPxv0mOiIsc4dE91RiUWfAUBmw+469EH3IWFQYMpuDtCmQPlHkrTmYu2K
gn1q0sLR6LAX/l9uQxGaSarW2ZXmrj4/dpsfmnRYS8zDDQw/0JQ=
=c954
-----END PGP SIGNATURE-----
```

⬅ By Date ➡ ⬅ By Thread ➡

Current thread:

APPLE-SA-2021-04-26-3 Security Update 2021-002 Catalina ***Apple Product Security via Fulldisclosure (Apr 27)***