APPLE-SA-2022-05-16-4 Security Update 2022-004 Catalina

From: Apple Product Security via Fulldisclosure <fulldisclosure () seclists org>
Date: Mon, 16 May 2022 16:20:22 -0700

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

APPLE-SA-2022-05-16-4 Security Update 2022-004 Catalina

Security Update 2022-004 Catalina addresses the following issues.
Information about the security content is also available at
https://support.apple.com/HT213255.

apache
Available for: macOS Catalina
Impact: Multiple issues in apache
Description: Multiple issues were addressed by updating apache to
version 2.4.53.
CVE-2021-44224
CVE-2021-44790
CVE-2022-22719
CVE-2022-22720
CVE-2022-22721

AppKit
Available for: macOS Catalina
Impact: A malicious application may be able to gain root privileges
Description: A logic issue was addressed with improved validation.
CVE-2022-22665: Lockheed Martin Red Team

AppleGraphicsControl
Available for: macOS Catalina
Impact: Processing a maliciously crafted image may lead to arbitrary
code execution
Description: A memory corruption issue was addressed with improved
input validation.
CVE-2022-26751: Michael DePlante (@izobashi) of Trend Micro Zero Day
Initiative

AppleScript
Available for: macOS Catalina
Impact: Processing a maliciously crafted AppleScript binary may
result in unexpected application termination or disclosure of process
memory
Description: An out-of-bounds read was addressed with improved input
```

validation.
CVE-2022-26697: Qi Sun and Robert Ai of Trend Micro

AppleScript
Available for: macOS Catalina
Impact: Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory
Description: An out-of-bounds read was addressed with improved bounds checking.
CVE-2022-26698: Qi Sun of Trend Micro

CoreTypes
Available for: macOS Catalina
Impact: A malicious application may bypass Gatekeeper checks
Description: This issue was addressed with improved checks to prevent unauthorized actions.
CVE-2022-22663: Arsenii Kostromin (0x3c3e)

CVMS
Available for: macOS Catalina
Impact: A malicious application may be able to gain root privileges
Description: A memory initialization issue was addressed.
CVE-2022-26721: Yonghwi Jin (@jinmo123) of Theori
CVE-2022-26722: Yonghwi Jin (@jinmo123) of Theori

DriverKit
Available for: macOS Catalina
Impact: A malicious application may be able to execute arbitrary code with system privileges
Description: An out-of-bounds access issue was addressed with improved bounds checking.
CVE-2022-26763: Linus Henze of Pinauten GmbH (pinauten.de)

Graphics Drivers
Available for: macOS Catalina
Impact: A local user may be able to read kernel memory
Description: An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation.
CVE-2022-22674: an anonymous researcher

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-2022-26720: Liu Long of Ant Security Light-Year Lab

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 read issue was addressed with improved input validation.
CVE-2022-26770: Liu Long of Ant Security Light-Year Lab

Intel Graphics Driver
Available for: macOS Catalina
Impact: An application may be able to execute arbitrary code with kernel privileges
Description: An out-of-bounds write issue was addressed with improved input validation.
CVE-2022-26756: Jack Dates of RET2 Systems, Inc

Intel Graphics Driver
Available for: macOS Catalina
Impact: A malicious application may be able to execute arbitrary code with kernel privileges
Description: A memory corruption issue was addressed with improved input validation.
CVE-2022-26769: Antonio Zekic (@antoniozekic)

Intel Graphics Driver
Available for: macOS Catalina
Impact: Processing maliciously crafted web content may lead to arbitrary code execution
Description: An out-of-bounds write issue was addressed with improved input validation.
CVE-2022-26748: Jeonghoon Shin of Theori working with Trend Micro Zero Day Initiative

Kernel
Available for: macOS Catalina
Impact: An application may be able to execute arbitrary code with kernel privileges
Description: A memory corruption issue was addressed with improved validation.
CVE-2022-26714: Peter Nguyễn Vũ Hoàng (@peternguyen14) of STAR Labs (@starlabs_sg)

Kernel
Available for: macOS Catalina
Impact: An application may be able to execute arbitrary code with kernel privileges
Description: A use after free issue was addressed with improved memory management.
CVE-2022-26757: Ned Williamson of Google Project Zero

libresolv
Available for: macOS Catalina
Impact: An attacker may be able to cause unexpected application termination or arbitrary code execution
Description: An integer overflow was addressed with improved input validation.
CVE-2022-26775: Max Shavrick (@_mxms) of the Google Security Team

LibreSSL
Available for: macOS Catalina
Impact: Processing a maliciously crafted certificate may lead to a denial of service
Description: A denial of service issue was addressed with improved input validation.
CVE-2022-0778

libxml2
Available for: macOS Catalina
Impact: A remote attacker may be able to cause unexpected application termination or arbitrary code execution
Description: A use after free issue was addressed with improved memory management.
CVE-2022-23308

OpenSSL
Available for: macOS Catalina
Impact: Processing a maliciously crafted certificate may lead to a denial of service
Description: This issue was addressed with improved checks.
CVE-2022-0778

PackageKit
Available for: macOS Catalina
Impact: A malicious application may be able to modify protected parts
of the file system
Description: This issue was addressed with improved entitlements.
CVE-2022-26727: Mickey Jin (@patch1t)

Printing
Available for: macOS Catalina
Impact: A malicious application may be able to bypass Privacy
preferences
Description: This issue was addressed by removing the vulnerable
code.
CVE-2022-26746: @gorelics

Security
Available for: macOS Catalina
Impact: A malicious app may be able to bypass signature validation
Description: A certificate parsing issue was addressed with improved
checks.
CVE-2022-26766: Linus Henze of Pinauten GmbH (pinauten.de)

SMB
Available for: macOS Catalina
Impact: An application may be able to gain elevated privileges
Description: An out-of-bounds write issue was addressed with improved
bounds checking.
CVE-2022-26715: Peter Nguyễn Vũ Hoàng of STAR Labs

SoftwareUpdate
Available for: macOS Catalina
Impact: A malicious application may be able to access restricted
files
Description: This issue was addressed with improved entitlements.
CVE-2022-26728: Mickey Jin (@patch1t)

TCC
Available for: macOS Catalina
Impact: An app may be able to capture a user's screen
Description: This issue was addressed with improved checks.
CVE-2022-26726: an anonymous researcher

Tcl
Available for: macOS Catalina
Impact: A malicious application may be able to break out of its
sandbox
Description: This issue was addressed with improved environment
sanitization.
CVE-2022-26755: Arsenii Kostromin (0x3c3e)

WebKit
Available for: macOS Catalina
Impact: Processing a maliciously crafted mail message may lead to
running arbitrary javascript
Description: A validation issue was addressed with improved input
sanitization.
CVE-2022-22589: Heige of KnownSec 404 Team (knownsec.com) and Bo Qu
of Palo Alto Networks (paloaltonetworks.com)

Wi-Fi
Available for: macOS Catalina
Impact: An application may be able to execute arbitrary code with
kernel privileges
Description: A memory corruption issue was addressed with improved

memory handling.
CVE-2022-26761: Wang Yu of Cyberserval

zip
Available for: macOS Catalina
Impact: Processing a maliciously crafted file may lead to a denial of service
Description: A denial of service issue was addressed with improved state handling.
CVE-2022-0530

zlib
Available for: macOS Catalina
Impact: An attacker may be able to cause unexpected application termination or arbitrary code execution
Description: A memory corruption issue was addressed with improved input validation.
CVE-2018-25032: Tavis Ormandy

zsh
Available for: macOS Catalina
Impact: A remote attacker may be able to cause arbitrary code execution
Description: This issue was addressed by updating to zsh version 5.8.1.
CVE-2021-45444

Additional recognition

PackageKit
We would like to acknowledge Mickey Jin (@patch1t) of Trend Micro for their assistance.

Security Update 2022-004 Catalina may be obtained from the Mac App Store or Apple's Software Downloads web site:
https://support.apple.com/downloads/
All information is also posted on the Apple Security Updates web site: https://support.apple.com/en-us/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-----

iQIzBAEBCAAdFiEEePiLW1MrMjw19XzoeC9qKD1prhgFAmKC1TYACgkQeC9qKD1p
rhjgGRAAggg84uE4zYtBHmo5Qz45wlY/+FT7bSyCyo2Ta0m3JQmm26UiS9ZzXlD0
58jCo/ti+gH/gqwU05SnaG88pSMT6VKaDDnmw8WcrPtbl6NN6JX8vaZLFLoGO0dB
rjwap7ulcLe7/HM8kCz3qqjKj4fusxckCjmm5yBMtuMklq7i51vzkT/+ws00ALcH
4S821CqIJlS2RIho/M/pih5A/H1Onw/nzKc7VOWjWMmmwoV+oiL4gMPE9kyIAJFQ
NcZO7s70Qp9N5Z0VGIkD5HkAntEqYGNKJuCQUrHS0fHFUxVrQcuBbbSiv7vwnOT0
NVcFKBQWJtfcqmtcDF8mVi2ocqUh7So6AXhZGZtL3CrVfNMgTcjq6y5XwzXMgwlm
ezMX73MnV91QuGp6KVZEmoFNlJ2dhKcJ0fYAhhW9DJqvJ1u5xIkQrUkK/ERLnWpE
9DIapT8uUbb9Zgez/tS9szv5jHhKtOoPbprju7d7LHw7XMFCVKbUvx745dFZx0AG
PLsJZQNsQZJIK8QdcLA50KrlyjR2ts4nUsKj07I6LR4wUmcaj+goXYq4Nh4WLnoF
x1AXD5ztdYlhqMcTAnuAbUYfuki0uzSy0p7wBiTknFwKMZNIaiToo64BES+7Iu1i
vrB9SdtTSQCMXgPZX1Al1e2F/K2ubovrGU9geAEwLMq3AKudI4g=
=JBHs
-----END PGP SIGNATURE-----

By Date By Thread

Current thread:

APPLE-SA-2022-05-16-4 Security Update 2022-004 Catalina ***Apple Product Security via Fulldisclosure (May 16)***