



Site Search

[Full Disclosure](#) mailing list archives[← By Date →](#) [← By Thread →](#)

List Archive Search



APPLE-SA-2021-09-20-8 Additional information for APPLE-SA-2021-09-13-4 Security Update 2021-005 Catalina

From: product-security-noreply--- via Fulldisclosure <fulldisclosure () seclists org>

Date: Mon, 20 Sep 2021 14:44:34 -0700

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

APPLE-SA-2021-09-20-8 Additional information for
APPLE-SA-2021-09-13-4 Security Update 2021-005 Catalina

Security Update 2021-005 Catalina addresses the following issues.
Information about the security content is also available at
<https://support.apple.com/HT212805>.

CoreGraphics

Available for: macOS Catalina

Impact: Processing a maliciously crafted PDF may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

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

CVE-2021-30860: The Citizen Lab

CoreServices

Available for: macOS Catalina

Impact: A sandboxed process may be able to circumvent sandbox restrictions

Description: An access issue was addressed with improved access restrictions.

CVE-2021-30783: an anonymous researcher, Ron Hass (@ronhass7) of Perception Point

Entry added September 20, 2021

CUPS

Available for: macOS Catalina

Impact: A local attacker may be able to elevate their privileges
Description: A permissions issue existed. This issue was addressed with improved permission validation.

CVE-2021-30827: an anonymous researcher

Entry added September 20, 2021

CUPS

Available for: macOS Catalina

Impact: A local user may be able to read arbitrary files as root
Description: This issue was addressed with improved checks.
CVE-2021-30828: an anonymous researcher
Entry added September 20, 2021

CUPS

Available for: macOS Catalina
Impact: A local user may be able to execute arbitrary files
Description: A URI parsing issue was addressed with improved parsing.
CVE-2021-30829: an anonymous researcher
Entry added September 20, 2021

curl

Available for: macOS Catalina
Impact: curl could potentially reveal sensitive internal information to the server using a clear-text network protocol
Description: A buffer overflow was addressed with improved input validation.
CVE-2021-22925
Entry added September 20, 2021

CVMS

Available for: macOS Catalina
Impact: A local attacker may be able to elevate their privileges
Description: A memory corruption issue was addressed with improved state management.
CVE-2021-30832: Mickey Jin (@patch1t) of Trend Micro
Entry added September 20, 2021

FontParser

Available for: macOS Catalina
Impact: Processing a maliciously crafted dfont file may lead to arbitrary code execution
Description: This issue was addressed with improved checks.
CVE-2021-30841: Xingwei Lin of Ant Security Light-Year Lab
CVE-2021-30842: Xingwei Lin of Ant Security Light-Year Lab
CVE-2021-30843: Xingwei Lin of Ant Security Light-Year Lab
Entry added September 20, 2021

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-2021-30835: Ye Zhang of Baidu Security
CVE-2021-30847: Mike Zhang of Pangu Lab
Entry added September 20, 2021

Kernel

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 memory handling.
CVE-2021-30830: Zweig of Kunlun Lab
Entry added September 20, 2021

Kernel

Available for: macOS Catalina
Impact: A malicious application may be able to execute arbitrary code with kernel privileges
Description: An out-of-bounds read was addressed with improved input validation.
CVE-2021-30865: Zweig of Kunlun Lab
Entry added September 20, 2021

Kernel

Available for: macOS Catalina

Impact: Mounting a maliciously crafted NFS network share may lead to arbitrary code execution with system privileges

Description: A race condition was addressed with additional validation.

CVE-2020-29622: Jordy Zomer of Certified Secure

Entry added September 20, 2021

Kernel

Available for: macOS Catalina

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

Description: A race condition was addressed with improved locking.

CVE-2021-30857: Zweig of Kunlun Lab

Entry added September 20, 2021

Kernel

Available for: macOS Catalina

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

Description: A type confusion issue was addressed with improved state handling.

CVE-2021-30859: Apple

Entry added September 20, 2021

libexpat

Available for: macOS Catalina

Impact: A remote attacker may be able to cause a denial of service
Description: This issue was addressed by updating expat to version 2.4.1.

CVE-2013-0340: an anonymous researcher

Entry added September 20, 2021

Preferences

Available for: macOS Catalina

Impact: An application may be able to access restricted files

Description: A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks.

CVE-2021-30855: Zhipeng Huo (@R3dF09) and Yuebin Sun (@yuebinsun2020) of Tencent Security Xuanwu Lab (xlab.tencent.com)

Entry added September 20, 2021

Sandbox

Available for: macOS Catalina

Impact: A user may gain access to protected parts of the file system
Description: An access issue was addressed with improved access restrictions.

CVE-2021-30850: an anonymous researcher

Entry added September 20, 2021

SMB

Available for: macOS Catalina

Impact: A remote attacker may be able to leak memory

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

CVE-2021-30844: Peter Nguyen Vu Hoang of STAR Labs

Entry added September 20, 2021

TCC

Available for: macOS Catalina

Impact: A malicious application may be able to bypass Privacy preferences

Description: A permissions issue was addressed with improved

validation.

CVE-2021-30713: an anonymous researcher

Entry added September 20, 2021

Additional recognition

Bluetooth

We would like to acknowledge say2 of ENKI for their assistance.

Entry added September 20, 2021

CoreML

We would like to acknowledge hjy79425575 working with Trend Micro Zero Day Initiative for their assistance.

Entry added September 20, 2021

CUPS

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

Entry added September 20, 2021

Kernel

We would like to acknowledge Anthony Steinhauser of Google's Safeside project for their assistance.

Entry added September 20, 2021

smbx

We would like to acknowledge Zhongcheng Li (CK01) for their assistance.

Entry added September 20, 2021

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-----

iQIzBAEBCAAAdFiEEePiLW1MrMjw19XzoeC9qKD1prhgFAMFI888ACgkQeC9qKD1p
rhhvSA/+MzMvNjUS7KUDdIBNgVfzpgGLGGy0ewyCCuLaTFGPptVVMlgXgo0Q1ds4
NQJ47AWXUk0EPotUdaMXYXTTLNRrS/rHuhrUar8tNgXV0uTIFoa0AaGNVFLbklxz
KRte/SqDIY7PdWobflBTeeR0lFq0/lIys+cyI3TtWezCGaGcdF00Ckhv76UFUUUi
qnB3hjxXVCkbwbetl6EMPQiiYp0zU8K0n95T3E24buR08CxNdWYbZ0kHqYaCAYLX
Fm0lPtX4VknTdwjwhMTmNrbrMmc7TP0LEUavTNv0ghslYbywX3Iwj6f2mC5ZArUB
klKZwLWPl8c0JmwMADnSpQc5VR+umM0fJdxsHajJu9/eWAuVK35IFJbQcZyP0Urv
N+B8V4tk9D+I1NmU+12QIALmUnnAmnzCBa/qE+FIGCyyBQgSM6WdmwXmWvQPX9/1
q7fVqW6zZv1A7z2Qal82sRkLH1APsoRGUQlw+uttmh6rKolpNgH4ZJ4Xhqcq/S4k
DgL85EvidWgaaTIj9+mI5NmqbY0E8/rkHtjxa0Y9wyjpWiw2rS07SXLTuDIRMBlt
hLBR20e5/ZqdKxxAE+U31ZI8PzJhEU4PoCL5xcciXxB0ilxhUgVLGDgmZol117Sy
+wX/g7wuaorhnCs0IWNBC/up76pBJlCe+ns0oWNPfdgP5qw2pZY=
=QJxi

-----END PGP SIGNATURE-----

Sent through the Full Disclosure mailing list

<https://nmap.org/mailman/listinfo/fulldisclosure>

Web Archives & RSS: <http://seclists.org/fulldisclosure/>

← [By Date](#) → ← [By Thread](#) →

Current thread:

APPLE-SA-2021-09-20-8 Additional information for APPLE-SA-2021-09-13-4 Security Update 2021-005 Catalina *product-security-noreply---* via *Fulldisclosure* (Sep 21)

Site Search



Nmap Security Scanner

[Ref Guide](#)

[Install Guide](#)

[Docs](#)

[Download](#)

[Nmap OEM](#)

Npcap packet capture

[User's Guide](#)

[API docs](#)

[Download](#)

[Npcap OEM](#)

Security Lists

[Nmap Announce](#)

[Nmap Dev](#)

[Full Disclosure](#)

[Open Source Security](#)

[BreachExchange](#)

Security Tools

[Vuln scanners](#)

[Password audit](#)

[Web scanners](#)

[Wireless](#)

[Exploitation](#)

About

[About/Contact](#)

[Privacy](#)

[Advertising](#)

[Nmap Public Source License](#)

