About the security content of Security Update 2021-005 Catalina

This document describes the security content of Security Update 2021-005 Catalina.

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 2021-005 Catalina

Released September 13, 2021

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

Core Telephony

Available for: macOS Catalina

Impact: A sandboxed process may be able to circumvent sandbox restrictions. Apple was aware of a report that this issue may have been actively exploited at the time of release.

Description: A deserialization issue was addressed through improved validation.

CVE-2021-31010: Citizen Lab and Google Project Zero

Entry added May 25, 2022

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: Nathan Nye of WhiteBeam Security, Inc.

Entry added September 20, 2021, updated May 25, 2022

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: Nathan Nye of WhiteBeam Security, Inc.

Entry added September 20, 2021, updated May 25, 2022

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: Nathan Nye of WhiteBeam Security, Inc.

Entry added September 20, 2021, updated May 25, 2022

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: Red Hat Product Security

Entry added September 20, 2021, updated May 25, 2022

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: Manish Bhatt of Red Team X @Meta, Zweig of Kunlun Lab

Entry added September 20, 2021, updated May 25, 2022

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

Published Date: November 06, 2023