

# About the security content of Security Update 2022-004 Catalina

This document describes the security content of Security Update 2022-004 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 2022-004 Catalina

Released May 16, 2022

### 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

### AppleEvents

Available for: macOS Catalina

Impact: A remote user may cause an unexpected app termination or arbitrary code execution

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

CVE-2022-22630: Jeremy Brown working with Trend Micro Zero Day Initiative

Entry added June 6, 2023

### **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: A remote user may be able to cause a denial-of-service

Description: This issue was addressed with improved checks.

CVE-2022-32790: Max Shavrick (@\_mxms) of the Google Security Team

Entry added June 21, 2022

#### **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: An app may be able to gain elevated privileges

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

CVE-2022-32794: Mickey Jin (@patch1t)

Entry added October 4, 2022

**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: Antonio Cheong Yu Xuan of YCISCQ

Entry updated June 6, 2023

### **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.


Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. [Contact the vendor](#) for additional information.

Published Date: November 02, 2023

Helpful?

Yes

No

 > Support > About the security content of Security Update 2022-004 Catalina

Copyright © 2026 Apple Inc. All rights reserved. [Privacy Policy](#) | [Terms of Use](#) | [Sales and Refunds](#) | [Site Map](#)

United States