About the security content of macOS Monterey 12.7.3

This document describes the security content of macOS Monterey 12.7.3.

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 releases page.

Apple security documents reference vulnerabilities by CVE-ID when possible.

For more information about security, see the Apple Product Security page.

macOS Monterey 12.7.3

Released January 22, 2024

Accessibility

Available for: macOS Monterey

Impact: An app may be able to access sensitive user data

Description: A privacy issue was addressed with improved private data redaction for log entries.

CVE-2023-42937: Noah Roskin-Frazee and Prof. J. (ZeroClicks.ai Lab)

Apple Neural Engine

Available for: macOS Monterey

Impact: An app may be able to execute arbitrary code with kernel privileges

Description: The issue was addressed with improved memory handling.

CVE-2024-23212: Ye Zhang of Baidu Security

curl

Available for: macOS Monterey

Impact: Multiple issues in curl

Description: Multiple issues were addressed by updating to curl version 8.4.0.

CVE-2023-38545

CVE-2023-38039

CVE-2023-38546

Entry updated February 13, 2024

ImageIO

Available for: macOS Monterey

Impact: Processing a maliciously crafted image may result in disclosure of process memory

Description: The issue was addressed with improved checks.

CVE-2023-42888: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Mail Search

Available for: macOS Monterey

Impact: An app may be able to access sensitive user data

Description: This issue was addressed with improved redaction of sensitive information.

CVE-2024-23207: Noah Roskin-Frazee and Prof. J. (ZeroClicks.ai Lab), and Ian de Marcellus

Power Manager

Available for: macOS Monterey

Impact: An app may be able to corrupt coprocessor memory

Description: The issue was addressed with improved checks.

CVE-2024-27791: Pan ZhenPeng (@Peterpan0927) of STAR Labs SG Pte. Ltd.

Entry added April 24, 2024

WebKit

Available for: macOS Monterey

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

Description: A type confusion issue was addressed with improved checks.

WebKit Bugzilla: 267134

CVE-2024-23222

Published Date: June 03, 2024