

# About the security content of macOS Ventura 13.6.4

This document describes the security content of macOS Ventura 13.6.4.

## 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 Ventura 13.6.4

Released January 22, 2024

### Apple Neural Engine

Available for: macOS Ventura

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

### Accessibility

Available for: macOS Ventura

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-Fraze and Prof. J. (ZeroClicks.ai Lab)

### Core Data

Available for: macOS Ventura

Impact: An app may be able to bypass Privacy preferences

Description: This issue was addressed by removing the vulnerable code.

CVE-2023-40528: Kirin (@Pwnrin) of NorthSea

### curl

Available for: macOS Ventura

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

### **Finder**

Available for: macOS Ventura

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

Description: The issue was addressed with improved checks.

CVE-2024-23224: Brian McNulty

### **ImageIO**

Available for: macOS Ventura

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

### **LoginWindow**

Available for: macOS Ventura

Impact: A local attacker may be able to view the previous logged in user's desktop from the fast user switching screen

Description: An authentication issue was addressed with improved state management.

CVE-2023-42935: ASentientBot

Entry updated April 24, 2024

### **Mail Search**

Available for: macOS Ventura

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

### **NSOpenPanel**

Available for: macOS Ventura

Impact: An app may be able to read arbitrary files

Description: An access issue was addressed with additional sandbox restrictions.

CVE-2023-42887: Ron Masas of BreakPoint.sh

### **Power Manager**

Available for: macOS Ventura

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 Ventura

**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

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: June 03, 2024

Helpful?

Yes

No

Apple > Support > About the security content of macOS Ventura 13.6.4