

HiveForce Labs

# THREAT ADVISORY



## VULNERABILITY REPORT

### **CVE-2025-43300: Zero-Day in Apple Image I/O Exploited in Targeted Attacks**

Date of Publication

August 22, 2025

Admiralty Code

A1

TA Number

TA2025257


# Summary

**First Seen:** August 20, 2025

**Affected Product:** Apple iOS, iPadOS, and macOS

**Impact:** CVE-2025-43300 is a critical zero-day flaw in Apple's Image I/O framework that allows attackers to execute code through a crafted image file, with little or no user interaction. Apple confirmed it is already being exploited in targeted attacks, making it a high-risk threat. Patches are available in iOS 18.6.2, iPadOS 18.6.2/17.7.10, and macOS Sequoia 15.6.1, Sonoma 14.7.8, and Ventura 13.7.8, users should update immediately to stay protected.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-43300	Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability	Apple iOS, iPadOS, and macOS			

# Vulnerability Details

## #1

CVE-2025-43300 is a critical zero-day vulnerability affecting Apple's Image I/O framework, which handles the processing of image file formats across iPhones, iPads, and Macs. The flaw is an out-of-bounds write issue that can corrupt memory and potentially allow attackers to execute malicious code on a device. Apple has confirmed that the vulnerability is already being exploited in highly targeted attacks, raising the urgency for users to update their systems immediately.

#2

The exploit is especially dangerous because it can be triggered with minimal or no user interaction, making it a potential “zero-click” attack. This means that simply receiving or processing a crafted image file could be enough to compromise a device. While current exploitation appears to be targeted, the severity of the vulnerability means it could be weaponized more widely if left unpatched.

#3

To mitigate the risk, Apple has released emergency updates in iOS 18.6.2, iPadOS 18.6.2 and 17.7.10, and macOS Sequoia 15.6.1, Sonoma 14.7.8, and Ventura 13.7.8. Users are strongly advised to install these patches immediately by checking the Software Update section on their devices.



## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-43300	macOS: All versions before macOS Sequoia 15.6.1, macOS Sonoma 14.7.8, and macOS Ventura 13.7.8. iOS and iPadOS: All versions before iOS/iPadOS 18.6.2 and 17.7.10.	cpe:2.3:o:apple:ipados:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*	CWE-787



# Recommendations



**Update Your Devices Immediately:** Install the latest patches released by Apple, including iOS 18.6.2, iPadOS 18.6.2/17.7.10, and macOS Sequoia 15.6.1, Sonoma 14.7.8, and Ventura 13.7.8. Confirm after updating that the system reflects the latest version to ensure the fix is applied correctly.



**Enable Automatic Updates:** Turn on automatic updates so your devices install security patches as soon as they are available. This reduces the window of exposure and ensures you're always protected against new threats.



**Be Cautious with Images and Media Files:** Avoid opening unsolicited images or files sent through email, messaging apps, or other untrusted sources. Since this flaw can be triggered with little to no interaction, even a simple preview could be dangerous.<sup>4</sup>



## Potential MITRE ATT&CK TTPs

<b><u>TA0002</u></b> Execution	<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0004</u></b> Privilege Escalation
<b><u>TA0040</u></b> Impact	<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1203</u></b> Exploitation for Client Execution
<b><u>T1588.005</u></b> Exploits	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1588.006</u></b> Vulnerabilities

## Patch Details

Apple fixed CVE-2025-43300 in iOS 18.6.2, iPadOS 18.6.2/17.7.10, and macOS Sequoia 15.6.1, Sonoma 14.7.8, Ventura 13.7.8, users should update via Software Update immediately.

Links:

<https://support.apple.com/en-us/124925>

<https://support.apple.com/en-us/124926>

<https://support.apple.com/en-us/124927>

<https://support.apple.com/en-us/124928>

<https://support.apple.com/en-us/124929>

## References

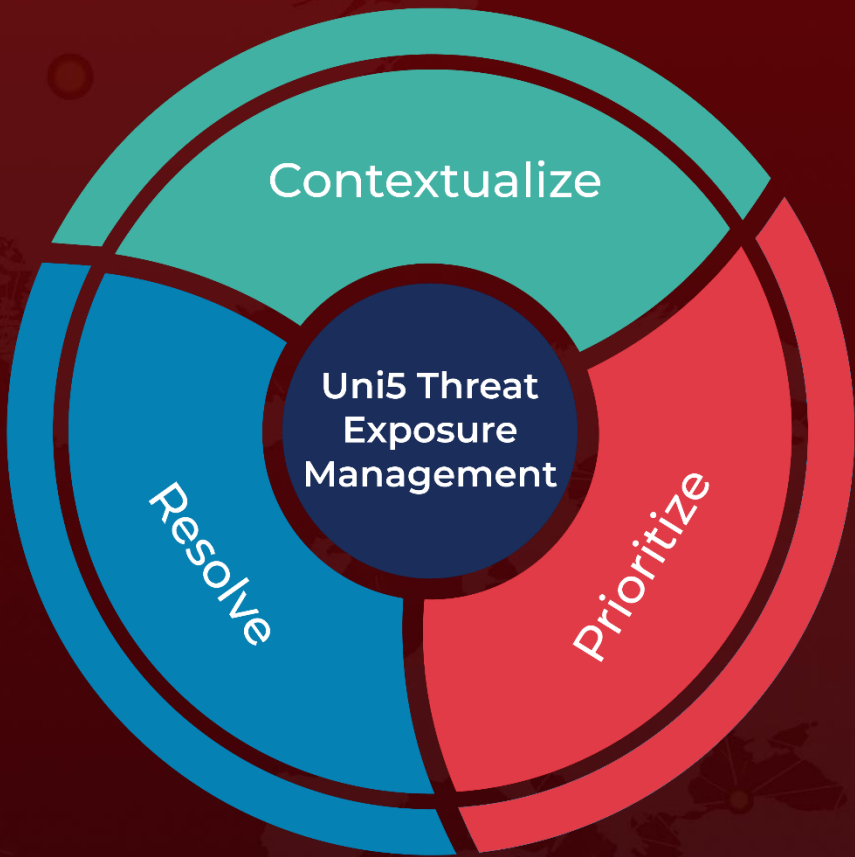
<https://threatprotect.qualys.com/2025/08/21/apple-addressed-zero-day-vulnerability-impacting-ios-ipados-and-macos-cve-2025-43300/>



# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON  
**August 22, 2025 • 4:10 AM**

