

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Apple Fixes Zero-Day Exploit That Bypasses USB Restricted Mode

Date of Publication

February 11, 2025

Admiralty Code

A1

TA Number

TA2025036


Summary

First Seen: February 10, 2025

Affected Products: Apple iOS and iPadOS

Impact: Apple has addressed a zero-day flaw in iOS and iPadOS that was actively exploited in highly sophisticated attacks. Tracked as CVE-2025-24200, this vulnerability allows attackers to bypass authorization checks and disable USB Restricted Mode on a locked device, potentially enabling cyber-physical attacks.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-24200	Apple iOS and iPadOS Incorrect Authorization Vulnerability	Apple iOS and iPadOS			

Vulnerability Details

#1

Apple has addressed a zero-day vulnerability, CVE-2025-24200, affecting iOS and iPadOS, which has been exploited in highly targeted, sophisticated attacks. The flaw arises from an authorization error that could allow attackers to disable USB Restricted Mode on a locked device, potentially enabling cyber-physical attacks.

#2

USB Restricted Mode is a critical security feature in iPhones and iPads that prevents unauthorized data access through USB accessories when a device has been locked for over an hour. By exploiting this vulnerability, attackers could bypass this protection, increasing the risk of unauthorized access.

#3

Apple has now patched the issue, and users are strongly advised to update their devices to the latest version to prevent potential exploitation. This comes shortly after Apple addressed another zero-day vulnerability, [CVE-2025-24085](#), which allowed malicious apps to escalate privileges on affected devices.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-24200	Apple iPadOS Version before 17.7.5, Apple iOS and iPadOS Version before 18.3.1	cpe:2.3:a:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	CWE-254

Recommendations



Stay Updated: Make sure your Apple devices are running the latest versions (iOS 18.3.1, iPadOS 18.3.1, or iPadOS 17.7.5) to fix the security flaw and stay protected from potential attacks.



Keep USB Restricted Mode On: Ensure this security feature remains enabled in settings to block unauthorized access through USB connections. Be cautious when connecting devices to unknown or untrusted USB ports or accessories.



Stay Alert for Suspicious Activity: Watch for unusual device behavior or unexpected USB connections, as these could signal an attempted exploit.



Enable Automatic Updates: Turn on automatic software updates by navigating to Settings > General > Software Update to ensure your device stays protected with the latest security patches.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0004</u> Privilege Escalation	<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities
<u>T1068</u> Exploitation for Privilege Escalation			

Patch Details

This vulnerability has been fixed in iPadOS 17.7.5, iOS 18.3.1, and iPadOS 18.3.1. To stay protected, update your device to the latest version as soon as possible.

Links: <https://support.apple.com/en-us/118575>

References

<https://support.apple.com/en-us/122174>

<https://support.apple.com/en-us/122173>

<https://hivepro.com/threat-advisory/Apple-Tackles-First-Zero-Day-of-2025-Actively-Exploited-in-the-Wild/>

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

February 11, 2025 • 4:20 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com