NATIONAL CSIRT CY

CVE-2025-24200

03/03/2025

USB Restricted Mode Bypass Vulnerability in Apple iOS & iPadOS

CONFIDENTIAL

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

Executive Summary

CVE-2025-24200 is a critical authorization vulnerability affecting Apple's iOS and iPadOS, allowing a physical attacker to bypass USB Restricted Mode on a locked device. USB Restricted Mode is a security feature designed to prevent unauthorized data access via the USB port after a device has been locked for an extended period. This flaw could enable sophisticated attackers to gain unauthorized access to sensitive data by disabling this protection.

https://www.cve.org/CVERecord?id=CVE-2025-24200

Analysis

The vulnerability in USB Restricted Mode, allowing an attacker with physical access to disable the feature. This could be exploited in high-risk scenarios, such as forensic investigations, theft, or targeted espionage. By bypassing USB restrictions, an attacker might gain access to device data or deploy additional exploits. The patch released by Apple strengthens security enforcement, closing the loophole. Since this flaw may have been used in real-world attacks, it is critical for all users—especially those handling sensitive data—to update their devices promptly and enable strong security measures.

Common Weakness Enumeration

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2025-24200

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-24200

Affected Systems

iPhone: iPhone XS and later

iPad Pro: 13-inch, 12.9-inch (3rd gen and later), 11-inch (1st gen and later)

iPad Air: 3rd generation and later

iPad: 7th generation and later

iPad Mini: 5th generation and later

Older iPads: iPad Pro 12.9-inch (2nd gen), iPad Pro 10.5-inch, iPad 6th generation

Solutions

Apple has released patches to address CVE-2025-24200 by improving state management. Users should immediately update their devices to the latest available versions to mitigate the risk of exploitation

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.