

GOVERNMENT OF THE REPUBLIC
OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



GOVERNEMENT DE LA
REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

13 March 2026

Advisory 121: Apple iOS and iPadOS Use-After-Free Vulnerability

Release Date: 05th March 2026
Impact: **HIGH / CRITICAL**
TLP: CLEAR

Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2023-41974 is a high-severity memory corruption vulnerability (CVSS 7.8) affecting Apple mobile operating systems. The flaw is classified as a Use-After-Free (CWE-416) vulnerability in the system's kernel memory management.

A *use-after-free* vulnerability occurs when a program continues to use a memory pointer after the memory has already been freed. This can lead to memory corruption, allowing attackers to manipulate system memory and potentially execute malicious code.

What are the systems affected?

The vulnerability affects Apple mobile operating systems prior to the patched release.

Affected platforms include:

- Apple iOS versions earlier than iOS 17
- Apple iPadOS versions earlier than iPadOS 17
- Apple iPhone and iPad devices running vulnerable OS versions

What does this mean?

The vulnerability requires local execution, meaning an attacker must get a malicious application onto the target device.

Typical attack vectors:

- 1. Delivery of a malicious application**
 - Attackers distribute a malicious or trojanized application through phishing, third-party app stores, or compromised software downloads.
- 2. Triggering the memory flaw**
 - The application interacts with vulnerable kernel components that improperly manage memory.
- 3. Use-after-free condition**
 - The system releases memory but continues referencing it.
- 4. Memory manipulation**
 - The attacker injects controlled data into the freed memory space.
- 5. Kernel-level code execution**
 - The malicious code executes with kernel privileges, bypassing normal application sandbox protections.

Mitigation process

CERTVU recommends the following:

1. Apply Security Updates Immediately

Apple addressed the vulnerability by improving memory management in newer operating systems.

Recommended update:

- Upgrade to iOS 17 or later
- Upgrade to iPadOS 17 or later

2. Restrict Untrusted Applications

- Install applications only from the official Apple App Store.
- Avoid sideloaded or unofficial applications that may contain malicious code.

3. Implement Mobile Device Security Controls

Organizations should:

- Use Mobile Device Management (MDM) solutions.

- Enforce minimum OS version requirements.
- Monitor devices for suspicious application behavior.

Reference

1. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
2. <https://www.cve.org/CVERecord?id=CVE-2023-41974>