Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apple Rolls Out Critical Updates to Address Zero-Day Flaws

Date of Publication	Admiralty Code	TA Number
March 6, 2024	A1	TA2024088

Summary

First Seen: March 2024
Affected Products: Apple devices
Impact: Apple has addressed two zero-day vulnerabilities in iOS, namely CVE-2024-23225 and CVE-2024-23296. These vulnerabilities were exploited in attacks targeting Mobile devices, providing attackers with arbitrary kernel read and write privileges, enabling them to bypass kernel memory protections.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-23225	Apple iOS and iPadOS Memory Corruption Vulnerability	iPadOS, Apple iOS	✓	✓	✓
CVE-2024-23296	Apple iOS and iPadOS Memory Corruption Vulnerability	iPadOS, Apple iOS	✓	✓	✓

Vulnerability Details

#1

Apple has published emergency security upgrades to address two actively exploited vulnerabilities, CVE-2024-23225 and CVE-2024-23296. These flaws in the iOS Kernel and RTKit allow attackers to circumvent kernel memory safeguards.

#2

An attacker with the ability to read and write to the kernel can circumvent memory protections by taking advantage of CVE-2024-23225. The OS kernel's boundary error is the cause of the vulnerability. On the target device, a malicious application can run arbitrary code and cause memory corruption.

#3 The RTKit real-time operating system (RTOS) has a memory corruption vulnerability called CVE-2024-23296, an attacker with unrestricted kernel read and write access may be able to get around kernel memory protections. This vulnerability results from a boundary issue in RTKit, which makes it possible for a malicious program to run arbitrary code and corrupt memory on the target machine.

#4 Apple has not disclosed details about current wild exploitation; but, state-sponsored spyware campaigns frequently leverage iOS zero-day vulnerabilities. Installing the security updates as soon as feasible is highly recommended to prevent prospective attack efforts.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-23225	iPadOS: 17.4 and prior, 16.7.6 and prior Apple iOS: 17.4 and prior, 16.7.6 and prior	cpe:2.3:a:apple:*:*:*:*:*:*:*	CWE-119
CVE-2024-23296	iPadOS: 17.4 and prior, 16.7.6 and prior Apple iOS: 17.4 and prior, 16.7.6 and prior	cpe:2.3:a:apple:*:*:*:*:*:*:*	CWE-119

Recommendations

Update Your Devices: Install the latest updates provided by Apple to address the CVE-2024-23225 and CVE-2024-23296 vulnerabilities. This update closes the security gap that allows attackers to exploit the vulnerability.

Revisit app permission: Periodically review the permissions granted to each app on your device. Check if all permissions are still necessary for the app to function properly. Disable permissions that are not essential for the app's core functionality.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0005 Defense Evasion	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1106 Native API	T1211 Exploitation for Defense Evasion	

Patch Details

Make sure to update your devices to the latest available versions to address these vulnerabilities:

iOS 17.4, iPadOS 17.4, iOS 16.7.6, and iPadOS 16.7.6.

References

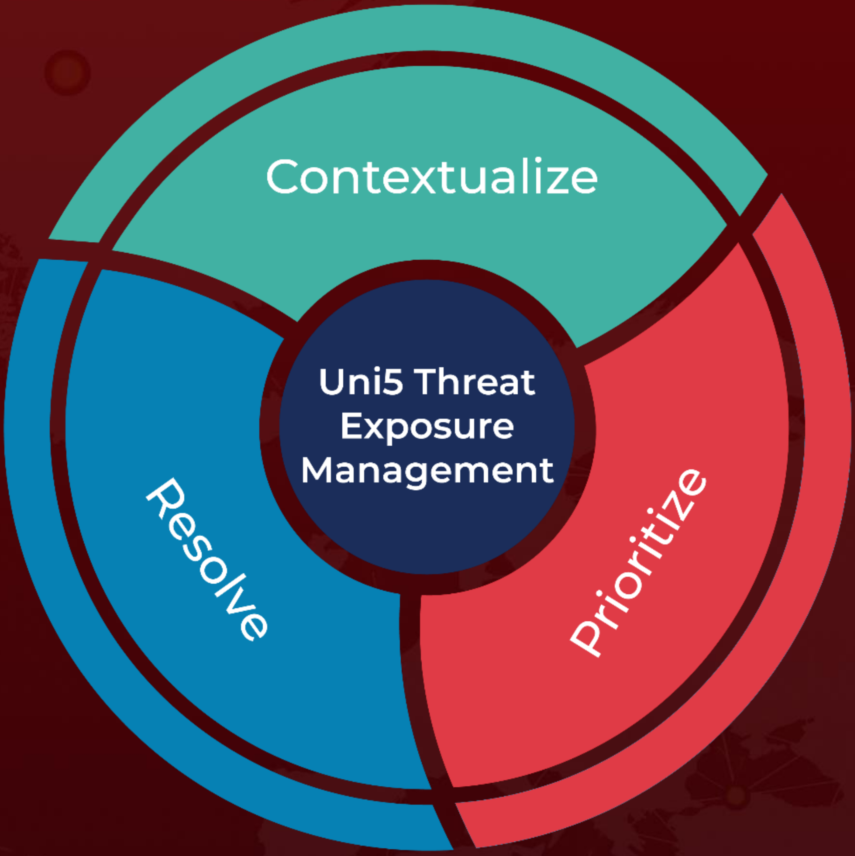
https://support.apple.com/en-us/HT214081

https://support.apple.com/en-us/HT214082

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

March 6, 2024 • 5:15 AM

More at www.hivepro.com