Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apple Addresses Two Zero-Day Flaws Exploited by Attackers

Date of Publication	Admiralty Code	TA Number
September 14, 2023	A1	TA2023371

Summary

First Seen: September 7, 2023
Affected Products: Apple iOS, iPadOS, watchOS and macOS
Impact: The two zero-day vulnerabilities (CVE-2023-41064 and CVE-2023-41061) enabling arbitrary code execution and system crashes. These vulnerabilities are actively exploited it poses severe risks, including data exposure and potential targeted attacks. Immediate patching and security vigilance are essential to mitigate these threats.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-41064	Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow Vulnerability	Apple iOS, iPadOS, and macOS	✓	✓	✓
CVE-2023-41061	Apple iOS, iPadOS, and watchOS Wallet Code Execution Vulnerability	Apple iOS, iPadOS, and watchOS	✓	✓	✓

Vulnerability Details

#1

An exploit chain, named BLASTPASS, capable of compromising iPhones running the latest iOS version without user interaction. The attack involves sending malicious images via PassKit attachments through iMessage. These vulnerabilities, identified as CVE-2023-41064 and CVE-2023-41061, targeted the ImageIO and Wallet frameworks within Apple's ecosystem.

#2

CVE-2023-41064 is a buffer overflow vulnerability within the ImageIO framework, which allows applications to process images. Attackers could exploit this flaw by sending a specially crafted image to a vulnerable device. If the manipulated image is processed, it can trigger a range of consequences, from crashing the device to executing malicious code.

#3

CVE-2023-41061, on the other hand, pertains to a validation issue within the Wallet framework. By sending a carefully crafted attachment to a targeted device, an attacker could exploit this vulnerability. If the victim opens the manipulated attachment, it could similarly lead to device crashes or the execution of arbitrary code.

#4

The reach of these vulnerabilities is extensive, impacting various Apple devices, ranging from older models to the latest releases. This includes iPhones starting from the iPhone 8, Apple Watches Series 4 and newer, Macs running macOS Ventura, and multiple generations of iPads and iPad Pros.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-41064	iPhone 8 and later iPad Pro (all models) iPad Air 3rd generation and later iPad 5th generation and later iPad mini 5th generation and later Macs running macOS Ventura	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	CWE-120
CVE-2023-41061	iPhone 8 and later iPad Pro (all models) iPad Air 3rd generation and later iPad 5th generation and later iPad mini 5th generation and later Apple Watch Series 4 and later	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*	CWE-20

Recommendations

Apply Security Patch and Updates: Ensure that your Apple devices, including iPhones, iPads, Macs, and Apple Watches, are regularly updated with the latest security patches and software updates. Apple typically releases patches quickly once vulnerabilities are discovered. Enabling automatic updates or regularly checking for updates and applying them as soon as they become available can significantly reduce your exposure to known vulnerabilities.

Exercise Caution with Unknown Attachments and Messages: Be cautious when receiving unsolicited messages, especially those containing attachments, from unknown or unexpected sources. Avoid opening or downloading attachments from untrusted senders, as these may contain malicious payloads that can exploit vulnerabilities. This practice is particularly relevant for email, messaging apps, and social media platforms.

Enable Security Features: Take advantage of built-in security features on your Apple devices. Consider enabling features such as Two-Factor Authentication (2FA) to add an extra layer of protection to your accounts. For iOS devices, consider activating "Lockdown Mode" if you believe you are at risk of targeted attacks. This feature can help block certain exploit chains, as mentioned in the context of CVE-2023-41064 and CVE-2023-41061.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
T1204 User Execution	T1204.002 Malicious File	T1588 Obtain Capabilities	T1588.005 Exploits
T1203 Exploitation for Client Execution	T1588.006 Vulnerabilities	T1204.003 Malicious Image	

Patch Details

upgrade to the most recent versions available below:

- macOS Ventura 13.5.2 for macOS Ventura
- iOS 16.6.1 for iPhone 8 and later
- iPadOS 16.6.1 for iPad Pro (all models), iPad Air 3rd generation and later, iPad 5th generation and later and iPad mini 5th generation and later
- watchOS 9.6.2 for Apple Watch Series 4 and later

Link:
https://support.apple.com/en-us/HT213905

https://support.apple.com/kb/HT213907

https://support.apple.com/en-us/HT213906

References

https://www.cisa.gov/news-events/alerts/2023/09/11/cisa-adds-two-known-vulnerabilities-catalog

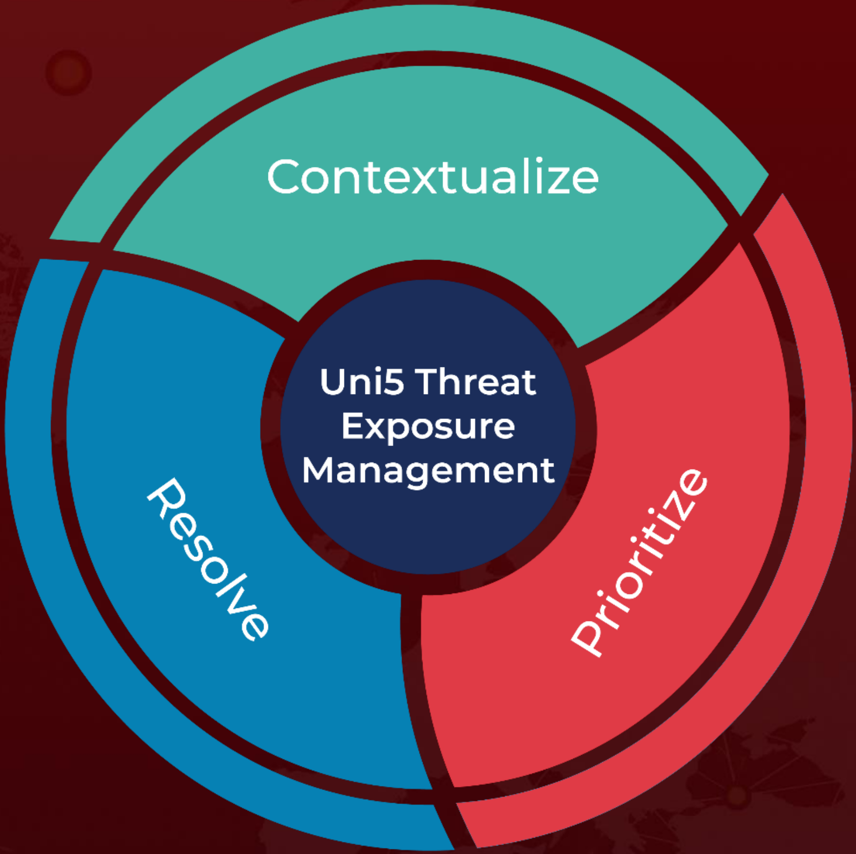
https://www.helpnetsecurity.com/2023/09/08/cve-2023-41064-cve-2023-41061/

https://www.csa.gov.sg/alerts-advisories/alerts/2023/al-2023-113

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

September 14, 2023 • 5:30 AM

More at www.hivepro.com