Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apple Tackles Zero-Day Flaws Impacting iPhones and Macs

Date of Publication	Admiralty Code	TA Number
July 25 , 2023	A1	TA2023311

Summary

First Seen: July 24, 2023
Affected Products: iOS, iPadOS, macOS, tvOS, and watchOS
Impact: Apple has addressed zero-day vulnerability that were exploited in targeted attacks on iPhones, Macs, and iPads.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-38606	Apple Buffer overflow Vulnerability	iOS, iPadOS, macOS, tvOS, and watchOS	✓	✗	✓

Vulnerability Details

#1

Apple has recently deployed comprehensive security updates across multiple platforms, such as iOS, iPadOS, macOS, tvOS, watchOS, and Safari, in response to various security vulnerabilities. Notably, one of these vulnerabilities tracked as CVE-2023-38606, has been actively exploited in the wild. This flaw resides in the kernel and has the potential to allow a malicious app to tamper with critical kernel components, presenting a serious security risk.

#2

The identified vulnerability enables a local application to exploit a privilege escalation, granting unauthorized access to system-level privileges. The root cause of this vulnerability lies in a boundary error within the OS kernel. By exploiting this flaw, a local application can trigger memory corruption, facilitating the execution of arbitrary code with elevated privileges.

#3

Notably, CVE-2023-38606 represents the third security vulnerability unearthed in correlation with "Operation Triangulation," an intricate mobile cyber espionage campaign that has been specifically targeting iOS devices since 2019, employing a sophisticated zero-click exploit chain. The campaign's modus operandi involves exploiting vulnerabilities without any user interaction, making it highly elusive and concerning.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-38606	iOS version before: 15.7.1. macOS version: 13.0 22A380 - 13.4.1 22F82, watchOS, tvOS	cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:-:*:*:*:*:*:*:*	CWE-119

Recommendations

Stay Updated and Apply Security Patches Promptly: Given the evolving landscape of cyber threats, it is essential for Apple users to stay vigilant and regularly update their iOS, iPadOS, macOS, tvOS, watchOS, and Safari to the latest versions. These updates often include critical security patches that protect against potential exploits, such as zero-day vulnerabilities. Promptly applying these **updates** will significantly reduce the risk of falling victim to cyberattacks.

Exercise Caution with Third-Party Apps: In light of the Operation Triangulation mobile cyber espionage campaign, it is advisable to exercise caution when installing and using third-party applications on Apple devices. Stick to trusted sources like the official App Store, as it provides an additional layer of security by screening apps for potential vulnerabilities and malware. Avoid sideloading apps from unknown sources, as they may pose significant risks to your device's security and privacy.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0040 Impact	T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	

Patch Details

In order to mitigate the vulnerability, it is imperative to Upgrade to macOS 13.5 or later.

Links:
https://support.apple.com/en-us/HT213843

https://support.apple.com/en-gb/HT213841

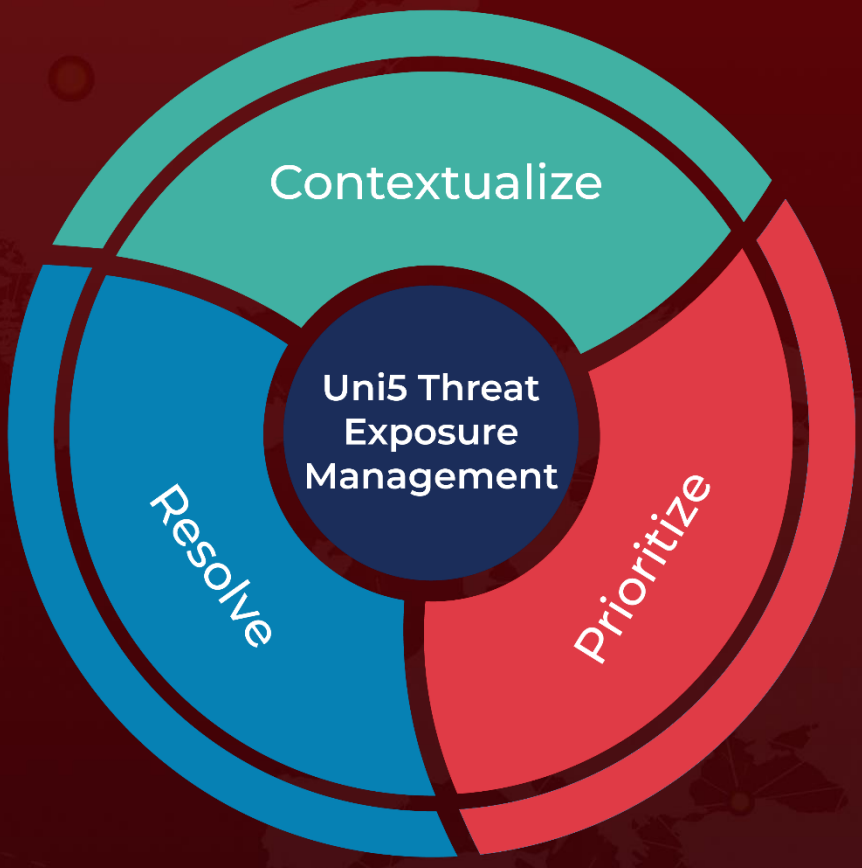
References

https://support.apple.com/en-in/HT201222

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

July 25, 2023 • 6:00 AM

More at www.hivepro.com