

HiveForce Labs

THREAT ADVISORY

 VULNERABILITY REPORT

Apple CoreGraphics Flaw Exploited in Targeted Attacks

Date of Publication

September 29, 2026

Admiralty Code

A1

TA Number

TA2026286

Summary

First Seen: September 2026

Affected Products: Apple iOS, iPadOS, macOS Tahoe, and macOS Sequoia

Impact: Apple has patched a serious flaw in CoreGraphics, the built-in framework that iPhones, iPads, and Macs use to draw images, graphics, and documents. Tracked as CVE-2026-86950 and reported by Meta Product Security, the bug is an out-of-bounds write that lets an attacker run their own code on a device simply by getting the target to open or process a specially crafted file. Apple says it is aware of a report that the flaw may already have been used in an extremely sophisticated attack aimed at specific, hand-picked individuals running iOS versions before iOS 27. The company released fixes on September 28, 2026 and has urged everyone to update right away.

CVE

CVE	NAME	AFFECTED PRODUCT	ZER O- DAY	CISA KEV	PATC H
CVE-2026-86950	Apple CoreGraphics Out-of-Bounds Write Vulnerability	Apple iOS, iPadOS, and macOS			

Vulnerability Details

#1

CVE-2026-86950 is an out-of-bounds write vulnerability (CWE-787) in CoreGraphics, the low-level Apple framework responsible for rendering graphics, images, and documents across iPhone, iPad, and Mac. The problem is a memory-safety error: when CoreGraphics parses a maliciously crafted file, it can write data beyond the boundary of the memory buffer set aside for it. Apple resolved the issue by adding improved bounds checking so the component can no longer write outside valid memory locations.

#2

Exploitation is client-side and file-based. An attacker builds a booby-trapped file and gets the victim's device to process it, whether by opening, previewing, or downloading it, which quietly triggers the vulnerable code path. If it works, the attacker gains arbitrary code execution inside the affected process, meaning they can run unauthorized commands, pull sensitive data, drop further malicious components, or set up a foothold for deeper compromise. The eventual damage depends on which application handled the file and what other weaknesses the attacker can chain onto it.

#3

The flaw affects iOS and iPadOS before 26.7.1, macOS Tahoe before 26.7.1, and macOS Sequoia before 15.8.1. Apple stated it is aware of a report that the issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 27, but it did not say how many people were targeted, whether any attempts succeeded, or when exploitation first began. The narrow, deliberate targeting is the signature of a well-resourced, surveillance-style operation rather than mass exploitation.

#4

The combination of low-interaction file processing, arbitrary code execution, and confirmed abuse places this firmly in the high-severity bracket. With CoreGraphics sitting in the file-processing path of countless everyday actions, and with Apple holding back attribution and indicators while its investigation continues, rapid patching should be treated as the primary line of defense.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-86950	Apple iOS and iPadOS (Before 26.7.1), Apple macOS Tahoe (Before 26.7.1), Apple macOS Sequoia (Before 15.8.1)	cpe:2.3:o:apple:iphone_os:*.~*.~*.~*.~*.~*~*, cpe:2.3:o:apple:ipados:*.~*.~*.~*.~*.~*~*, cpe:2.3:o:apple:macos:*.~*.~*.~*.~*.~*~*	CWE-787

Recommendations



Update Your Apple Devices Immediately: Install the latest updates without delay, iOS 26.7.1 and iPadOS 26.7.1 on iPhone and iPad, macOS Tahoe 26.7.1, and macOS Sequoia 15.8.1 on Mac. On mobile devices you can do this through Settings, then General, then Software Update. This patch closes the vulnerability, and updating is the fastest way to protect a device.



Give High-Risk Users Extra Protection: Since this flaw was used against specifically chosen individuals, prioritize people who are common surveillance targets, such as executives, journalists, activists, and government staff. For these users, turn on Lockdown Mode, which sharply reduces the attack surface for exactly this style of targeted, file-based exploitation.



Confirm Patch Coverage Across the Fleet: Use your mobile device management platform to verify that updates have actually reached every managed Apple device, and flag any that are still running older iOS, iPadOS, or macOS versions. Follow up on stragglers directly so no unpatched device slips through.



Be Careful With Untrusted Files: Until every device is patched, treat unexpected files, especially images and documents from unknown or unsolicited senders, with caution, and avoid opening or previewing them. Because the attack only needs a device to process a crafted file, user awareness meaningfully lowers the risk during the patch window.



Vulnerability Management: Regularly assess and update software to address known vulnerabilities, and keep an accurate inventory of operating system versions and applied patches. Building a fast, reliable patch cycle, particularly for exploited flaws like this one, shrinks the window attackers have to work with.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1566</u> : Phishing	<u>T1566.001</u> : Spearphishing Attachment
Execution	<u>T1203</u> : Exploitation for Client Execution	
	<u>T1204</u> : User Execution	<u>T1204.002</u> : Malicious File
	<u>T1059</u> : Command and Scripting Interpreter	
Resource Development	<u>T1588</u> : Obtain Capabilities	<u>T1588.006</u> : Vulnerabilities



Patch Links

<https://support.apple.com/en-us/149226>

<https://support.apple.com/en-us/149228>

<https://support.apple.com/en-us/149229>



References

<https://support.apple.com/en-us/149229>

<https://support.apple.com/en-us/149228>

<https://support.apple.com/en-us/149226>

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 Demo of HivePro.

REPORT GENERATED ON

September 29, 2026 • 08:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com