Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apple Zero-Day Exploited in Targeted Attacks (CVE-2026-20700)

Date of Publication	Admiralty Code	TA Number
February 13, 2026	A1	TA2026043

Summary

First Seen: February 11, 2026
Affected Products: Apple iOS, iPadOS, macOS Tahoe, tvOS, watchOS, visionOS (dyld component)
Impact: Apple has released emergency security updates addressing CVE-2026-20700, a critical zero-day memory corruption vulnerability in dyld, Apple's Dynamic Link Editor, responsible for loading and linking dynamic libraries across all Apple platforms. The vulnerability has been confirmed as actively exploited in an extremely sophisticated attack campaign targeting specific high-profile individuals on iOS versions before iOS 26. The flaw allows an attacker who has achieved memory write capability to execute arbitrary code by corrupting dyld's state during library loading, effectively hijacking control flow to run malicious shellcode. Apple addressed the vulnerability with improved state management in iOS 26.3, iPadOS 26.3, macOS Tahoe 26.3, watchOS 26.3, tvOS 26.3, and visionOS 26.3.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20700	Apple Multiple Buffer Overflow Vulnerability	Apple iOS, iPadOS, macOS Tahoe, tvOS, watchOS, visionOS	✓	✓	✓

Vulnerability Details

#1

CVE-2026-20700 is a memory corruption vulnerability residing in Apple's dyld (Dynamic Link Editor), the system component responsible for loading dynamic libraries into memory and bridging application code with system frameworks at runtime. The flaw stems from improper state management within the dyld component. Apple addressed the root cause through improved state management mechanisms in the patched versions.

#2

The vulnerability allows an attacker who has already achieved memory write capability on a target device to leverage the flaw in dyld to execute arbitrary code. This means the exploitation requires an initial access vector, such as a separate vulnerability or exploit chain, to gain the prerequisite memory write primitive before CVE-2026-20700 can be triggered.

#3

The exploit undermines Apple's entire chain of trust, since dyld is the first component that runs when any application launches. Compromising it enables the attacker to inject and execute payloads before runtime protections such as code signing verification, sandboxing, and ASLR are fully initialized, effectively bypassing the foundational security mechanisms that all subsequent layers of defense depend upon.

#4

The affected products span the full range of Apple's operating system ecosystem, including iOS and iPadOS, macOS Tahoe, tvOS, watchOS, and visionOS.

#5

Apple has confirmed that CVE-2026-20700 has been actively exploited in the wild in what the company describes as an "extremely sophisticated attack against specific targeted individuals." The vulnerability is part of a broader exploitation chain, with two additional CVEs, CVE-2025-14174 (an out-of-bounds memory access in webkit) and CVE-2025-43529 (a use-after-free vulnerability in WebKit), also issued in response to the same attack report and previously patched in December 2025. Google Threat Analysis Group, which focuses on government-backed cyber threats, discovered and reported all three vulnerabilities, reinforcing the likelihood of advanced threat actor involvement.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-20700	Apple iOS (Before 26.3), Apple iPadOS (Before 26.3), Apple macOS Tahoe (Before 26.3), Apple tvOS (Before 26.3), Apple watchOS (Before 26.3), Apple visionOS (Before 26.3)	cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:*	CWE-119

Recommendations

Apply Apple Security Updates Immediately: Update all Apple devices to the latest patched versions, including iOS 26.3 and iPadOS 26.3, macOS Tahoe 26.3, watchOS 26.3, tvOS 26.3, and visionOS 26.3. Given the confirmed active exploitation, this patch should be treated as an emergency update across all organizational Apple device fleets. Coordinate with MDM (Mobile Device Management) solutions to push updates to managed devices without delay.

Verify Patch Coverage Across All Device Categories: Confirm that all Apple devices within the organization, including less commonly managed devices such as Apple TVs and Apple Watches, are running the remediated OS versions. Devices running older OS branches (iOS 18.7.5, iPadOS 18.7.5, macOS Sequoia 15.7.4, macOS Sonoma 14.8.4) should be monitored closely for backported fixes and updated as soon as patches become available for those branches.

Enable Automatic Updates on All Apple Devices: Ensure that automatic software update settings are enabled across all organizational and personal Apple devices to reduce the window of exposure for future zero-day vulnerabilities. This is particularly important for devices that are not managed through enterprise MDM solutions.

Prioritize High-Value Targets for Immediate Remediation: Given that the exploitation was described as targeting specific individuals with sophisticated attacks, prioritize patching for devices belonging to executives, government officials, journalists, human rights workers, and other individuals who may be at elevated risk of targeted surveillance campaigns.

Conduct Post-Patch Security Assessment: Review security logs and endpoint telemetry for indicators of compromise related to dyld exploitation or anomalous code execution behavior on Apple devices. Given the exploit chain involves multiple vulnerabilities (CVE-2025-14174, CVE-2025-43529, and CVE-2026-20700), also verify that the December 2025 patches addressing the prior two CVEs are applied.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub Technique
Execution	T1203: Exploitation for Client Execution	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1211: Exploitation for Defense Evasion	
	T1574: Hijack Execution Flow	T1574.004: Dylib Hijacking
		T1574.006: Dynamic Linker Hijacking
Initial Access	T1189: Drive-by Compromise	

Patch Links

https://support.apple.com/en-us/126346

https://support.apple.com/en-us/126348

https://support.apple.com/en-us/126351

https://support.apple.com/en-us/126352

https://support.apple.com/en-us/126353

References

https://support.apple.com/en-us/126346

https://support.apple.com/en-us/126348

https://support.apple.com/en-us/126351

https://support.apple.com/en-us/126352

https://support.apple.com/en-us/126353

https://www.helpnetsecurity.com/2026/02/12/apple-zero-day-fixed-cve-2026-20700/

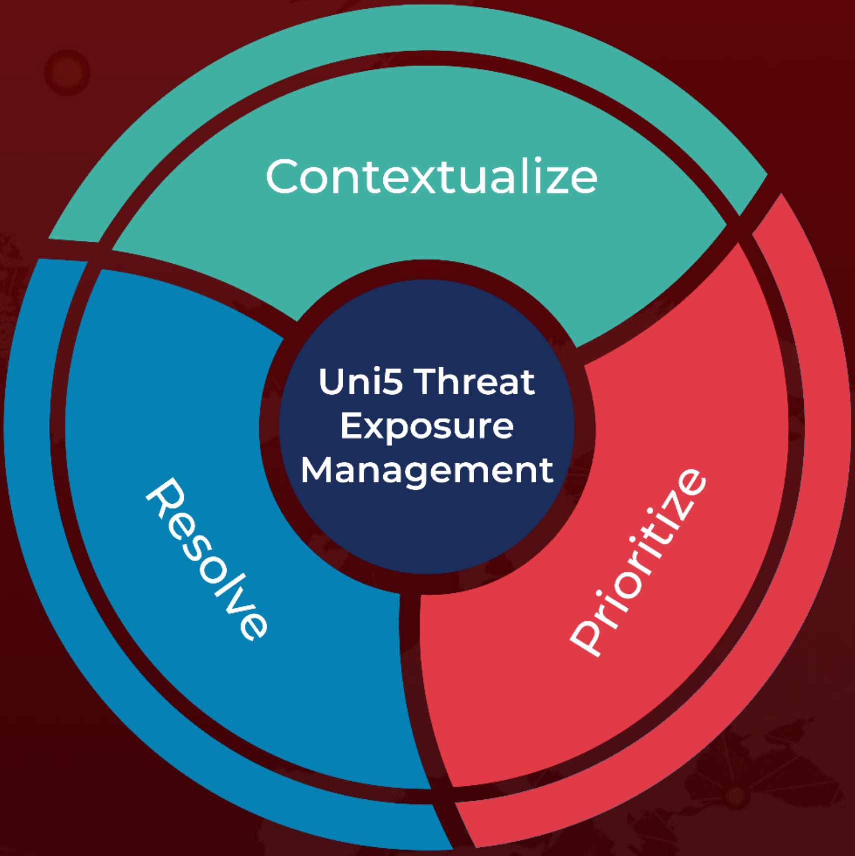
https://hivepro.com/threat-advisory/apple-webkit-zero-days-exploited-in-the-wild/

https://hivepro.com/threat-advisory/google-chrome-zero-day-exploited-in-angle-graphics-engine/

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

February 13, 2026 ● 08:13 AM

More at www.hivepro.com