Apple's Most Secure iPhones Ever — This Is Why You Should Upgrade

Summary

Apple's new iPhone 17 and iPhone Air feature "Memory Integrity Enforcement" (MIE), a significant upgrade to memory safety. MIE leverages Apple's silicon and OS to provide always-on memory safety protection, making exploit chains more difficult and expensive for attackers. This upgrade aims to redefine the landscape of memory safety for Apple products.

Zak Doffman Sep 11, 2025 at 12:11pm EDT

Is this the real reason to upgrade?
Getty Images

It wasn't the highlight of Apple's iPhone 17 and iPhone Air launch event. But it's more important than new colors, sizes and cameras. Apple has confirmed the new iPhone has one of "the most significant upgrades" in the "history of consumer operating systems." And if you're wavering on whether or not to upgrade, this could be the tipping point.

The last 12 months has seen warning after warning as industrial spyware targets iPhone and Android devices. Excepting nation-state attacks, most of the headline zero-day vulnerabilities exploited in the wild have the spyware industry behind the scenes.

…

Meet Apple's new "Memory Integrity Enforcement," which the iPhone-maker says "is the culmination of an unprecedented design and engineering effort." In short, MIE leverages Apple's own silicon and OS to deliver "always-on memory safety protection."

Most "mercenary spyware" attacks targeting iPhones "share a common denominator with those targeting Windows and Android: they exploit memory safety vulnerabilities, which are interchangeable, powerful, and exist throughout the industry."

Apple says that "based on our evaluations pitting MIE against exceptionally sophisticated mercenary spyware attacks from the last three years," it believes this "will make exploit chains significantly more expensive and difficult to develop and

maintain, disrupt many of the most effective exploitation techniques from the last 25 years, and completely redefine the landscape of memory safety for Apple products."

…

Memory exploitation targets a weakness in how a device reads from or writes to memory, allowing an attacker to destabilize a system and execute their own code. Put simply, it opens a remote door into part of a device that should not be accessible.

Sophisticated attacks chain together different exploits — one might open the door to planting code while another might be a weakness in an app or service that can then be compromised. A third might power what can then be done on a device, accessing data, intercepting messages and communicating with remote command and control.

Apple is locking down the initial access point. "Because of how dramatically it reduces an attacker's ability to exploit memory corruption vulnerabilities on our devices, we believe Memory Integrity Enforcement represents the most significant upgrade to memory safety in the history of consumer operating systems."

ForbesMicrosoft's Surface Pro Mistake — The 'Ultimate' Ad For Apple's iPadBy Zak Doffman

MIE tags sections of a device's memory, enabling the hardware to check the integrity of any memory access request. It works because Apple controls the hardware and OS. Only Google has the same security potential in the Android world.

A week from now, we'll know how good this generational upgrade is once security analysts get to test the update for themselves.