Researchers break Apple's new MacBook pro weeks after release

November 21 2023

Credit: CC0 Public Domain

A Georgia Tech researcher has successfully evaded security measures on Apple's latest MacBook Pro with the M3 processor chip to capture his fictional target's Facebook password and second-factor authentication

text.

By the end of his demonstration video, Ph.D. student Jason Kim showed how the recently discovered iLeakage side-channel exploit is still a genuine threat to Apple devices, regardless of how updated their software might be.

First discovered by Kim and Daniel Genkin, an associate professor in the School of Cybersecurity and Privacy, the vulnerability affects all recent iPhones, iPads, laptops, and desktops produced by Apple since 2020.

iLeakage allows attackers to see what's happening on their target's Safari browser. This vulnerability allows potential access to Instagram login credentials, Gmail inboxes, and YouTube watch histories, as Kim demonstrated last month on a slightly older MacBook Pro.

"A remote attacker can deploy iLeakage by hosting a malicious webpage they control, and a target just needs to visit that webpage," said Kim. "Because Safari does not properly isolate webpages from different origins, the attacker's webpage is able to coerce Safari to put the target webpage in the same address space. The attacker can use speculative execution to subsequently read arbitrary secrets from the target page."

How is this possible? Well, as manufacturers developed faster and more efficient CPUs, their devices have become vulnerable to something called speculative execution attacks. This vulnerability is in the design of the chip itself. It has led to major software issues since the Spectre attack was reported in 2018.

There have been many attempts to stop these types of attacks, but Kim and Genkin show through their research that more work still needs to be done.

"iLeakage shows these attacks are still relevant and exploitable, even after nearly six years of Spectre mitigation efforts following its discovery," said Genkin. "Spectre attacks coerce CPUs into speculatively executing the wrong flow of instructions. We have found that this can be used in several different environments, including Google Chrome and Safari."

The team made Apple aware of its findings on Sept. 12, 2022. Since then, the tech company has issued mitigation for iLeakage in Safari. However, the researchers note that the update was not initially enabled by default. It was only compatible with macOS Ventura 13.0 and higher as of today.

So far, the team does not have evidence that real-world cyber-attackers have used iLeakage. They've determined that iLeakage is a significantly difficult attack to orchestrate end-to-end, requiring advanced knowledge of browser-based side-channel attacks and Safari's implementation.

The vulnerability is confined to the Safari web browser on macOS because the exploit leverages peculiarities unique to Safari's JavaScript engine. However, iOS users face a different situation due to the sandboxing policies on Apple's App Store. The policies require other browser apps using iOS to use Safari's JavaScript engine, making nearly every browser application listed on the App Store vulnerable to iLeakage.

iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices will be published at the 2023 ACM SIGSAC Conference on Computer and Communications Security later this month.

More information: iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices. ileakage.com/