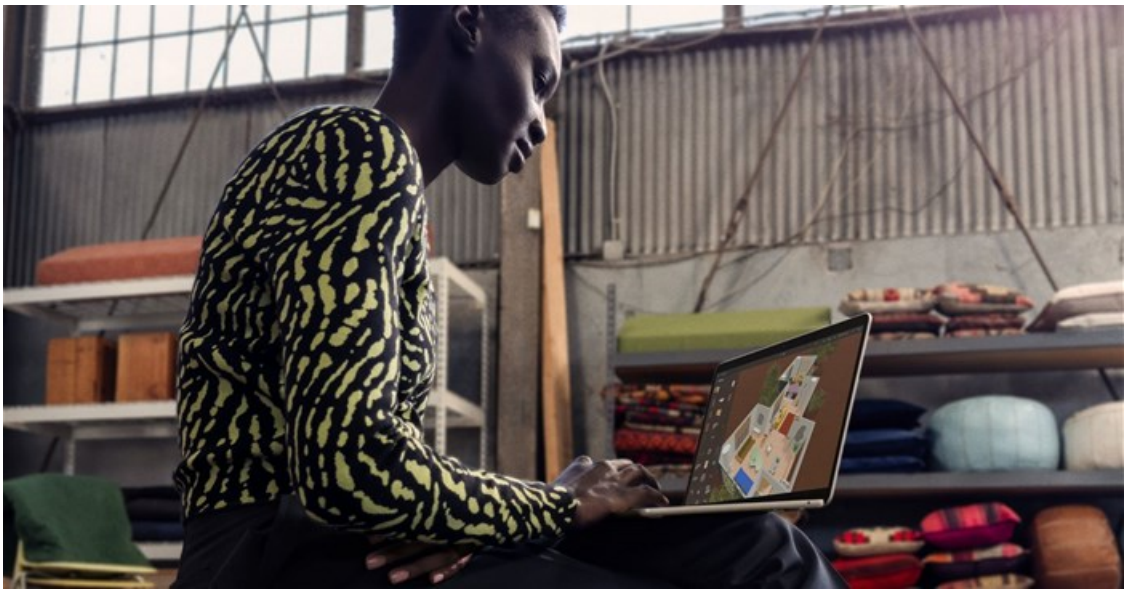
How the 'GoFetch' attack could target your Mac

By Lindsey Schutters

25 Mar 2024

A newly discovered security flaw called *GoFetch* has Apple device users concerned. It's a sophisticated attack that targets the way recent Apple devices (those with M1, M2, M3, or A14 chips) handle information. Think of it like a program sneakily peeking into your computer's temporary memory to steal sensitive data involved in password protection and other security measures.



Apple has found success with its Macs after moving to homebaked silicon because of the incredible battery endurance. Source: Apple Newsroom

Why does it matter? If successful, GoFetch could allow hackers to extract secret login details and other highly secure information from your Mac. The exploit targets the CPU's on-chip data memory-dependent prefetcher (DMP) and is relatively unfixable on older processors.

How difficult is it? While serious, it's not a simple attack. It takes significant technical skill and the ability to run a malicious program on your device.

Qualcomm sets sights on Apple M2 laptops with Snapdragon X Elite

Lindsey Schutters 25 Oct 2023

How it works

Memory hunt Apple's M-series processors try to be helpful by predicting what data you might need next and loading it in advance. GoFetch exploits this feature.

Hunting for secrets The attack program looks for patterns in this pre-loaded data, things that resemble the way secure cryptographic keys (think of them like ultra-complex passwords) are constructed.

Timing is everything GoFetch uses precise timing measurements to extract bits and pieces of those security keys, essentially piecing them together over time.

While the GoFetch attack can potentially extract cryptographic keys from systems using Apple CPUs, it doesn't directly relate to the functionality of Touch ID. There's also no information available that suggests the GoFetch attack can be used to bypass Apple ID authentication or break into a Mac.

Are you at risk?

The flaw is specific to Apple's M1-series and A14 chips, so Intel-based Macs and other devices aren't affected.

The attack needs a malicious program running directly on your Mac. This isn't something that can easily happen remotely.

This isn't something the average person needs to lose sleep over, but staying vigilant is always wise. IT departments overseeing enterprise Mac fleets, however, should caution users about malicious actors.

Protect yourself

While the vulnerability is tied to hardware function and design, Apple is likely working on a fix for the M3 processors – which can have the DMP turned off. Users should install security updates as soon as possible.

Avoid downloading software from dodgy sources or opening suspicious attachments – basic cybersecurity is still key.

If you handle particularly sensitive information on your Mac, consulting a cybersecurity expert might provide peace of mind.

GoFetch is a reminder no device is completely invulnerable. Awareness and smart practices are your best defence.

ABOUT LINDSEY SCHUTTERS

Lindsey is the editor for ICT, Construction&Engineering and Energy&Mining at Bizcommunity

- DCDT overhauls radio frequency spectrum policy - 31 May 2024
- Vodacom goes to war against spectrum pooling - 30 May 2024
- Icasa extends deadline for digital migration regulations review - 27 May 2024
- HPE takes aim at Cisco, emphasises partner ecosystem and AI focus - 24 May 2024
- OpenAI inks News Corp deal, Google threatens to cut news funding - 23 May 2024

View my profile and articles...