

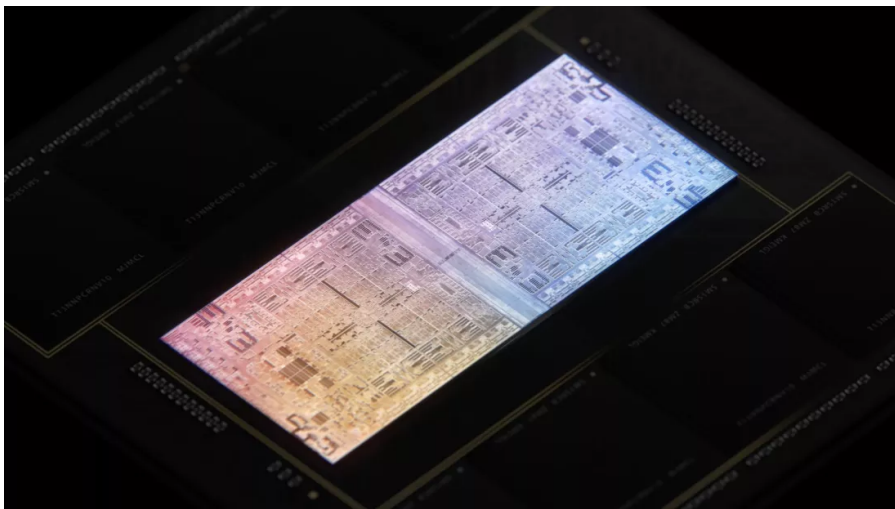


HARDWARE SECURITY APPLE APPLE SILICON

"Augury" vulnerability discovered in Apple silicon and mobile chips

Researchers say it isn't too serious, yet

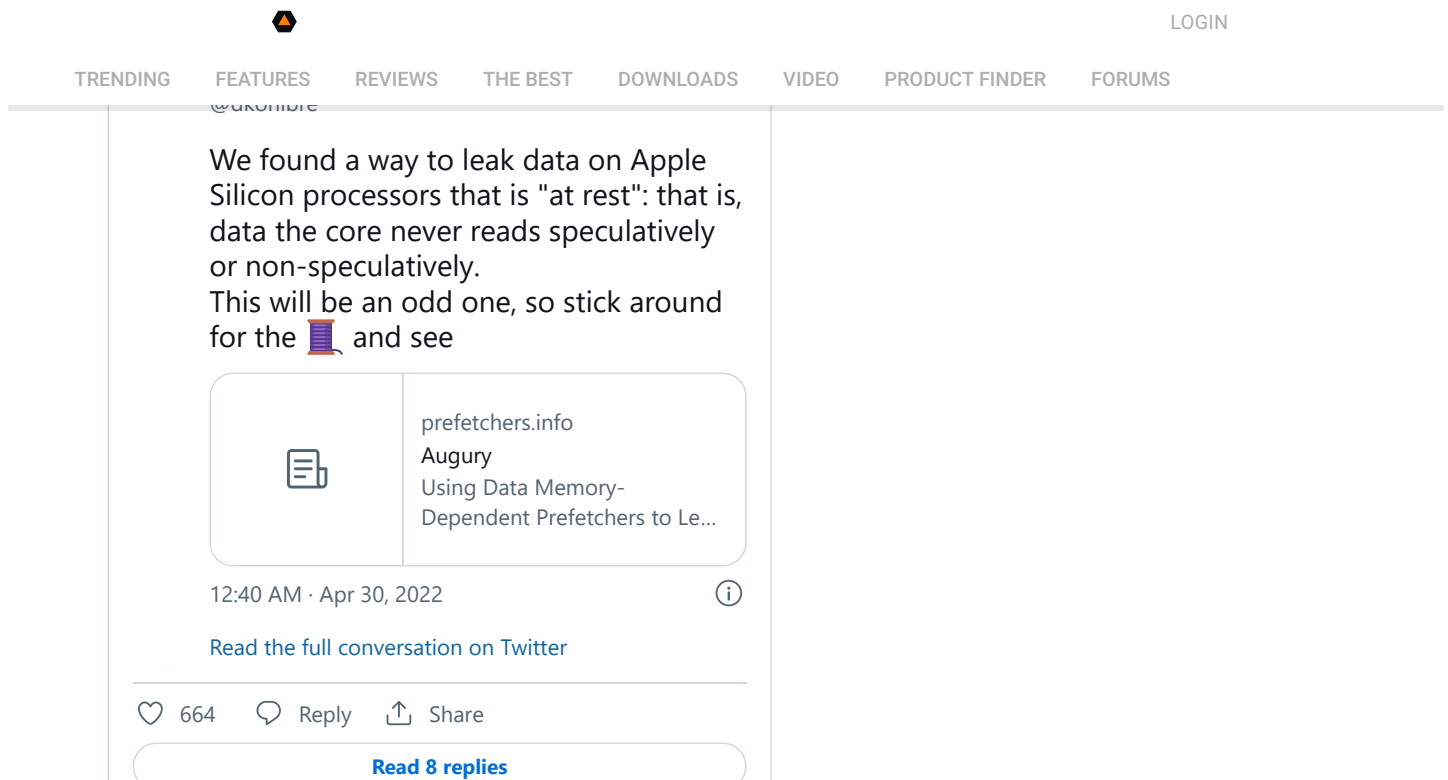
By [Daniel Sims](#) May 3, 2022, 2:18 PM



Why it matters: Hardware-based security flaws like Spectre have been a serious issue for Intel and AMD since their discovery in 2018. Now one has emerged for Apple's latest custom processors. Although not as serious as Spectre, it confirms that Apple silicon isn't immune to vulnerabilities.

Researchers recently [published](#) a paper detailing a vulnerability they are calling Augury that affects Apple's M1, M1 Max, and A14 processors. It might also reach older A-series chips and newer M1 relatives.

Although Augury hasn't led to real exploits yet, it's unique because it can leak data that neither the core nor any instructions have read. This nullifies many defenses against [Spectre](#) which work by tracking what data the core and instructions access.



Augury comes from Apple silicon's use of a Data Memory-Dependent Prefetcher (DMP) which is an optimization that accounts for the content of previous memory prefetches. That method provides a clue as to the memory's contents, making it possible to leak them.

The researchers don't think Augury is very dangerous partly because it only prefetches valid virtual addresses. However, it can break ASLR (Address Space Layout Randomization), which could be the first step in a serious exploit.

The authors of the paper sent Apple all the details on Augury before publishing their findings, so the company could provide a fix if it ever becomes a problem.

3 comments

59 interactions

Share this article:

Related Stories

- Apple iPhone 14 Pro may house autofocus front camera in a hole-punch cutout
- Indie classic Darwinia receives major overhaul for "10,000th anniversary"
- Global smartphone shipments fall 11%, but Samsung and Apple grew their market share

2022 Road to Readiness Roadshow

What if great sales reps could be created, not just hired?
Join us to learn how to create more top performers.

REGISTER