Apple's Safari browser is still vulnerable to Spectre attacks, researchers show

October 26 2023

Credit: Unsplash/CC0 Public Domain

Modern processors come with a fundamental vulnerability in their hardware architecture that allows attackers to hijack sensitive data. This insight emerged from the so-called Spectre attack reported in 2018.

A great number of devices and operating systems were affected. In response, manufacturers developed countermeasures—Apple was one of

them. Still, researchers showed even in 2023 that Mac and iOS systems are not yet adequately protected against this type of attack.

A team from Ruhr University Bochum (Germany), Georgia Tech and the University of Michigan showed that they could exploit the hardware vulnerability to gain access to passwords, emails and location data via the Safari browser. Apple has released first software updates that aim at fixing the vulnerability and continues to work on further updates. On the website ileakage.com, the researchers report about the vulnerability, available updates and how they can be enabled.

The project was conducted jointly by Professor Yuval Yarom from the Cluster of Excellence "Cyber Security in the Age of Large-Scale Adversaries" (CASA) in Bochum, Jason Kim and Associate Professor Daniel Genkin from Georgia Tech and Stephan van Schaik from the University of Michigan. They will present their findings at the Conference on Computer and Communications Security (CCS), which will take place in Copenhagen from 26 to 30 November 2023.

Gaining access to passwords and email accounts

In order to execute the new attack called "iLeakage," attackers must first direct users to a website that they control. "Users can't tell that they've landed on such a page," explains Yuval Yarom from the Faculty of Computer Science at Ruhr University Bochum. His advice: "As always, the rule is that you should only click on trustworthy sites."

If a user visits the attacker's website, the attacker can open the user's email app in a new window and read the contents of the inbox. Or they can open other websites, for example the login page of the user's bank. "We also showed that the attacker could automatically use the login data stored in the password manager LastPass if the auto-fill option is enabled," says Yuval Yarom. This is how even supposedly securely

stored passwords could be hacked.

Security gap in hardware architecture

The security gap results from the operating principle of modern processors (CPUs). When a CPU receives a series of instructions, it doesn't execute them one after another, but runs them simultaneously. Sometimes, instructions that require certain conditions to be met are initiated even if it's not yet clear whether these conditions do apply.

This speculative approach speeds up the system. The CPU estimates which condition is likely to apply and starts the process that is probably required. If it turns out that the precondition hasn't been met, the CPU discards the process and restarts it. However, discarded processes leave traces in the system, and this is precisely where the vulnerability lies. Attackers can extract sensitive memory data from such changes in the system.

Vendors have integrated countermeasures into their browsers as protection against this form of side-channel attack. In Safari, for example, each web page accessed by the user is supposed to be run in a separate process. However, the researchers showed that they could bypass the defense and open a second web page in the same process. This would allow attackers to intercept information that should in fact be unattainable.

More information: iLeakage: Browser-based timerless speculative execution attacks on Apple devices, Conference on Computer and Communications Security (CCS) 2023, Copenhagen, Denmark, paper download: ileakage.com/files/ileakage.pdf

Provided by Ruhr-Universitaet-Bochum