Despite fix, Apple has yet to address WebKit security bug affecting iPhone and MacOS

May 28 2021, by Sarah Katz

Apple logo. Credit: Unsplash.com

While a fix emerged three weeks ago for the security bug affecting the WebKit browser engine used by Apple products such as iPhone and Mac, Apple has yet to implement the fix. Researchers at the security

firm Theori have found that this WebKit vulnerability mainly causes Safari to crash. However, following a re-check after the supplied fix, they discovered that the bug still remains on both iOS and MacOS.

"Patch-gapping" is the term for the time period between when a fix becomes available and the application of that fix to affected systems and products. In this case, Theori cautions Apple about waiting too long to make use of the fix for the WebKit browser, lest attackers have more time and opportunity to compromise impacted systems.

This vulnerability was caused by a confusion bug taking advantage of AudioWorklet, the interface allowing developers to alter, control, render and play audio with the lowest possible latency. Unfortunately, attackers can exploit this vulnerability to remotely execute evil code on affected devices.

That said, attackers using this vulnerability on WebKit would still have to circumvent Pointer Authentication Codes (PAC), an exploit mitigation system wherein users must input the correct cryptographic signature before code can be rendered in memory. That means that in the absence of either this signature or some kind of a bypass, attackers will fortunately not be able to run their malicious code.

Researchers have confirmed that this exploit builds arbitrary read/write primitives which attackers could use to build a chain of further exploits. Moreover, they stated that PAC bypass methods count as a distinct issue that should be disclosed separately.

Thus far, six of the eight Apple exploits already uncovered in 2021 alone have been found to involve the WebKit browser engine.

More information: blog.theori.io/research/webkit-type-confusion/