Webkit zero-day exploit besieges Mac and iOS users with malvertising redirects

Enlarge / Artist’s impression of a malicious hacker coding up a BlueKeep-based exploit.

reader comments

36 with 32 posters participating, including story author

Share this story

Attackers have bombarded the Internet with more than 1 billion malicious ads in less than two months. The attackers targeted iOS and macOS users with what were zero-day vulnerabilities in Chrome and Safari browsers that were recently patched, researchers said on Monday.

More than 1 billion malicious ads served in the past six weeks contained exploit code that redirected vulnerable users to malicious sites, according to a post published by security firm Confiant. The surge of malicious ads exploited a Safari vulnerability in both iOS and macOS, as well as a Chrome vulnerability in iOS.

“Staggering volume”

“If we take a snapshot of eGobbler activity from August 1 to September 23, 2019, then we see a staggering volume of impacted programmatic impressions,” Confiant researcher and engineer Eliya Stein wrote. “By our estimates, we believe up to 1.16 billion impressions have been affected.”

To generate successful redirects, eGobbler was exploiting what had been a zero-day vulnerability in Webkit, the browser engine used in Safari and that shares code with Blink, the Webkit fork used for Chrome. The vulnerability existed in a JavaScript function (known as the onkeydown event,) which occurs each time a user presses a key on the keyboard. Tracked as CVE-2019-8771, the vulnerability allowed ads linked in HTML tags known as iframes to break out of security sandbox protections that prevent a user from being redirected without explicitly initiating it.

Enlarge / One of the malvertisements eGobbler served in the recent campaign.

“The nature of the bug is that a cross-origin nested iframe is able to ‘autofocus’ which bypasses the ‘allow-top-navigation-by-user-activation’ sandbox directive on the parent frame,” Stein wrote. “With the inner frame automatically focused, the

keydown event becomes a user-activated navigation event, which renders the ad sandboxing entirely useless as a measure for forced redirect mitigation.”

Confiant privately reported a vulnerability to both the Google and Apple security teams on August 7. The vulnerability was fixed in Chrome with the September 19 release of iOS 13. The Safari patch landed five days later with the release of Safari 13.0.1. This Webkit bugtracker entry shows that the flaw has been fixed in the underlying browser engine on August 9.

The blast of malicious ads comes five months after a similar eGobbler campaign served an estimated 500 million malicious ads. That blitz also relied on a then-unpatched vulnerability in the iOS version of Chrome. Tracked as CVE-2019–5840, that flaw was fixed in June with the release of Chrome 75.

The latest campaign concentrated on phishing pages, including the one shown above and to the right, that served spoofed custom messaging based on the target’s mobile provider. Countries in Europe were heavily targeted in this recent wave, which is why the images are not in English.

https://arstechnica.com/?p=1577215