Forbes Middle East

‘Hundreds Of Millions’ Of iPhones Vulnerable To New ‘Unfixable’ Hack

A new vulnerability in Apple’s iOS operating system is sitting on hundreds of millions of iPhones, iPads and iPods, according to the researcher who found it. As a result, hackers are now salivating at the prospect of being able to remove Apple’s control over their devices and load whatever software they like, breathing new life into the old art of so-called jailbreaking.

The hack has been dubbed checkm8 by a researcher who goes by the name axi0mX, who described the hack as “a permanent unpatchable bootrom exploit for hundreds of millions of iOS devices.” That means hackers can take the code released by axi0mX on Github and potentially load firmware (the core of the operating system) onto an iPhone. In turn, that means they have stripped Apple’s control away from the device and could do what they wanted on it, though some additional exploits would be required.

“Most generations of iPhones and iPads are vulnerable: from iPhone 4S (A5 chip) to iPhone 8 and iPhone X (A11 chip),” axi0mX wrote on Twitter. But the risk to users is limited: The researcher said that the vulnerability could “only be triggered over USB and requires physical access. It cannot be exploited remotely.”

Jailbreak excitement

However, it has got a subculture of the securty community excited. With some more tweaks, the exploit could be used to “jailbreak” an iPhone. A jailbreak uses what are known as “exploit chains,” by which various vulnerabilities are used to take control of an iPhone. In doing so, Apple’s control over the device is removed. That allows the user (or jailbreaker) to put whatever software they want on the device, though they might not get the same updates and security protections Apple offers a normal user.

Luca Todesco, one of the world’s more famous jailbreakers, said he’d looked at the exploit and said an imminent jailbreak was likely, while also confirming the latest iOS vulnerability could not be patched. “A full jailbreak requires some extra work in patches. ... although it's not hard. The hard part was being able to load patched firmware, which you now can,” he told *Forbes*over an encrypted messenger.

“It’s not a full jailbreak just yet. It can be developed into a full jailbreak.”

Axi0mX was certainly excited about the potential, adding: “This is possibly the biggest news in iOS jailbreak community in years. I am releasing my exploit for free for the benefit of iOS jailbreak and security research community.”

Apple hadn’t responded to a request for comment at the time of publication.

https://www.forbesmiddleeast.com/hundreds-of-millions-of-iphones-vulnerable-to-new-unfixable-hack