Issued 11/16/18

Fixed Facebook Privacy Bug Could Have Allowed Bad Actors to Steal Personal Info

Back in May 2018, Facebook patched a vulnerability which could allow malicious actors to collect user profile information by taking advantage of a cross-site request forgery (CSRF) security issue. Imperva's Ron Masas discovered the bug while looking for loopholes and vulnerabilities threat actors could exploit to access Facebooks users' personal information and reported it to Facebook via their responsible disclosure program. The issue was found by Masas while he was perusing "Facebook's online search results, and in their HTML noticed that each result contained an iframe element — probably used for Facebook's own internal tracking. Being pretty familiar with the unique cross-origin behavior of iframes." Attackers could have exploited the security issue by crafting malicious web pages which it had to trick Facebook users to visit and click on. Following any click event on the maliciously crafted page, a new tab or popup would be automatically opened executing a Facebook search with a custom query previously prepared by the attacker. "Since the number of iframe elements on the page reflects the number of search results, we can simply count them by accessing the fb.frames.length property," said Masas in his analysis. "By manipulating Facebook's graph search, it's possible to craft search queries that reflect personal information about the user."