13-The Verge-Facebook

Email

Illustration by Alex Castro / The Verge

A previously reported Facebook vulnerability was similarly found in the company’s Messenger product, according to security research group Imperva. Nearly a year ago, Imperva researchers discovered that, through Messenger, a hacker could use “any website to expose who you have been messaging with.” The bug was disclosed to Facebook in November and subsequently patched.

Hackers could target a Facebook user’s web browser and exploit iframe elements to see which friends the user had talked to and which were not in the user’s contact list. Imperva confirmed the hackers couldn’t gain any other data from the attack.

Like the vulnerability in Facebook reported last November , Messenger users would have been vulnerable if they visited a malicious site with Chrome and then clicked on the site while they were still logged in on Facebook. That would give the hackers access to run any queries on a new Facebook tab and extract personal data.

You would need to visit a malicious site and be logged into Facebook to be vulnerable

After Imperva disclosed the issue to Facebook, the company tried to issue a fix by randomizing iframe elements, an HTML element vital to the vulernability. But later, Imperva pointed out that a hacker could still design an algorithm that would continue to expose user’s contacts. Facebook then removed iframes from Messenger entirely. Facebook told The Verge in a statement: “We appreciate the researcher’s submission to our bug bounty program. The issue in his report stems from the way web browsers handle content embedded in webpages and is not specific to Facebook.”

“Browser-based side channel attacks are still an overlooked subject,” Israel-based Imperva researcher Ron Masas writes in the report. “While big players like Facebook and Google are catching up, most of the industry is still unaware.” Masas noted that while the technique wasn’t common yet, it could “increase in popularity throughout 2019” as it typically didn’t leave a trace.

Over the past few years, Facebook has come under fire for rampant privacy violations and mishandling of user data. From the Cambridge Analytica scandal reported last March to a data breach Facebook revealed in October, millions of users have had their data leaked. The news of today’s vulnerability also comes a day after Facebook CEO Mark Zuckerberg announced plans to merge Messenger, WhatsApp, and Instagram into a service that would combine its products through a single backend, positioning the move as a pivot to a “privacy-focused communications platform.”

Update March 7th, 11:23PM ET: This article was updated with comment from Facebook. Facebook also noted the bug was reported in November, not May.

By signing up, you agree to our Privacy Notice and European users agree to the data transfer policy.

Subscribe