kathrynglickman, Facebook Newsroom

An Update on the Security Issue

10h ago

By Guy Rosen, VP of Product Management

We have been working around the clock to investigate the security issue we discovered and fixed two weeks ago so we can help people understand what information the attackers may have accessed. Today, we're sharing details about the attack we've found that exploited this vulnerability. We have not ruled out the possibility of smaller-scale attacks, which we're continuing to investigate.

As we've said, the attackers exploited a vulnerability in Facebook's code that existed between July 2017 and September 2018. The vulnerability was the result of a complex interaction of three distinct software bugs and it impacted "View As," a feature that lets people see what their own profile looks like to someone else. It allowed attackers to steal Facebook access tokens, which they could then use to take over people's accounts. Access tokens are the equivalent of digital keys that keep people logged in to Facebook so they don't need to re-enter their password every time they use the app.

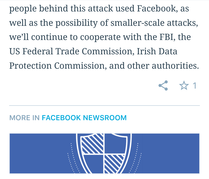
Here's how we found the attack that exploited this vulnerability. We saw an unusual spike of activity that began on September 14, 2018, and we started an investigation. On September 25, we determined this was actually an attack and identified the vulnerability. Within two days, we closed the vulnerability, stopped the attack, and secured people's accounts by resetting the access tokens for people who were potentially exposed. As a precaution, we also turned off "View As." We're cooperating with the FBI, which is actively investigating and asked us not to discuss who may be behind this attack.

We now know that fewer people were impacted than we originally thought. Of the 50 million people whose access tokens we believed were affected, about 30 million *actually* had their tokens stolen. Here's how it happened:

First, the attackers already controlled a set of accounts, which were connected to Facebook friends. They used an automated technique to move from account to account so they could steal the access tokens of those friends, and for friends of those friends, and so on, totaling about **400,000 people.** In the process, however, this technique automatically loaded those accounts' Facebook profiles, mirroring what these 400,000 people would have seen when looking at their own profiles. That includes posts on their timelines, their lists of friends, Groups they are members of, and the names of recent Messenger conversations. Message content was not available to the attackers, with one exception. If a person in this group was a Page admin whose Page had received a message from someone on Facebook, the content of that message was available to the attackers.

The attackers used a portion of these 400,000 people's lists of friends to steal access tokens for about 30 million people. For **15 million people**, attackers accessed two sets of information – name and contact details (phone number, email, or both, depending on what people had on their profiles). For **14 million people**, the attackers accessed the same two sets of information, as well as other details people had on their profiles. This included username, gender, locale/language, relationship status, religion, hometown, self-reported current city, birthdate, device types used to access Facebook, education, work, the last 10 places they checked into or were tagged in, website, people or Pages they follow, and the 15 most recent searches. For **1 million people**, the attackers did not access any information.

People can check whether they were affected by visiting our Help Center. In the coming days, we'll send customized messages to the 30 million people affected to explain what information the attackers might have accessed, as well as steps they can take to help protect themselves, including from suspicious emails, text messages, or calls.



Customized messages that people will see depending on how they were impacted.

This attack did not include Messenger, Messenger Kids, Instagram, WhatsApp, Oculus, Workplace, Pages, payments, third-

people behind this attack used Facebook, as well as the possibility of smaller-scale attacks, we'll continue to cooperate with the FBI, the US Federal Trade Commission, Irish Data Protection Commission, and other authorities.

MORE IN FACEBOOK NEWSROOM

Security Update

Security Update Additional Technical Details Morning Press Call Transcript Afternoon Press Call Transcript Originally published on September 2

Facebook Login Update

By Guy Rosen, VP of Product Management We wanted to provide an update on the security attack that we announced last week. This was a seriou

MORE ON WORDPRESS.COM

Straylite

Up to 50 millon FACEBOOK accounts breached in attack...

Up to 50 mn Facebook accounts breached in attack San Francisco (AFP) – Facebook revealed on Fri

Ashley E. Tillery
CW39 Houston

Facebook says attack exposed info of 50 million users

An attack on Facebook discovered earlier this week exposed information on nearly 50 million of the