A New Facebook Bug Exposes Millions of Email Addresses

A recently discovered vulnerability discloses user email addresses even when they're set to private.

Dan Goodin, Ars Technica   04.22.2021 08:00 AM

Photograph: MirageC/Getty Images

Still smarting from last month's dump of phone numbers belonging to 500 million Facebook users, the social media giant has a new privacy crisis to contend with: a tool that, on a massive scale, links Facebook accounts with their associated email addresses, even when users choose settings to keep them from being public.

This story originally appeared on Ars Technica, a trusted source for technology news, tech policy analysis, reviews, and more. Ars is owned by WIRED's parent company, Condé Nast.

A video circulating on Tuesday showed a researcher demonstrating a tool named Facebook Email Search v1.0, which he said could link Facebook accounts to as many as 5 million email addresses per day. The researcher—who said he went public after Facebook said it didn't think the weakness he found was "important" enough to be fixed—fed the tool a list of 65,000 email addresses and watched what happened next.

"As you can see from the output log here, I'm getting a significant amount of results from them," the researcher said as the video showed the tool crunching the address list. "I've spent maybe $10 to buy 200-odd Facebook accounts. And within three minutes, I have managed to do this for 6,000 [email] accounts."

Ars obtained the video on condition the video not be shared. A full audio transcript appears at the end of this post.

In a statement, Facebook said: "It appears that we erroneously closed out this bug bounty report before routing to the appropriate team. We appreciate the researcher sharing the information and are taking initial actions to mitigate this issue while we follow up to better understand their findings."

A Facebook representative didn't respond to a question asking if the company told the researcher it didn't consider the vulnerability important enough to warrant a fix. The representative said Facebook engineers believe they have mitigated the leak by disabling the technique shown in the video.

The researcher, whom Ars agreed not to identify, said that Facebook Email Search exploited a front-end vulnerability that he reported to Facebook recently but that "they [Facebook] do not consider to be important enough to be patched." Earlier this year, Facebook had a similar vulnerability that was ultimately fixed.

"This is essentially the exact same vulnerability," the researcher says. "And for some reason, despite me demonstrating this to Facebook and making them aware of it, they have told me directly that they will not be taking action against it."

Facebook has been under fire not just for providing the means for these massive collections of data, but also for actively promoting the idea that they pose minimal risk to Facebook users. An email that the company inadvertently sent to a reporter at the Dutch publication DataNews instructed public relations people to "frame this as a broad industry issue and normalize the fact that this activity happens regularly." Facebook has also made the distinction between scraping and hacks or breaches.

It's not clear if anyone actively exploited this bug to build a massive database, but it certainly wouldn't be surprising. "I believe this to be quite a dangerous vulnerability, and I would like help in getting this stopped," the researcher said.

Here's the written transcript of the video:

So, what I would like to demonstrate here is an active vulnerability within Facebook, which allows malicious users to query email addresses within Facebook, and have Facebook return any matching users.

This works with a front-end vulnerability with Facebook, which I've reported to them, made them aware of, um, that they do not consider to be important enough to be patched—which I would consider to be quite a significant privacy violation and a big problem.

This method is currently being used by software which is available right now within the hacking community.

Currently it's being used to compromise Facebook accounts for the purpose of taking over Pages groups and, uh, Facebook advertising accounts for obviously monetary gain. I've set up this visual example within no JS.

What I've done here is I've taken 250 Facebook accounts, newly registered Facebook accounts, which I've purchased online for about $10.

I have queried or I'm querying 65,000 email addresses. And as you can see from the output log here, I'm getting a significant amount of results from them.

If I have a look at the output file, you can see I have a user ID name and the email address matching the input email addresses, which I have used. Now I have, as I say, I've spent maybe $10 to buy 200-odd Facebook accounts. And within three minutes, I have managed to do this for 6,000 accounts.

I have tested this at a larger scale, and it is possible to use this to extract *feasibly up to 5 million email addresses per day.*

Now there was an existing vulnerability with Facebook earlier this year, which was patched. This is essentially the exact same vulnerability. And for some reason, despite me demonstrating this to Facebook and making them aware of it, they have told me directly that they will not be taking action against it.

So I am reaching out to people such as yourselves, in hope that you can use your influence or contacts to get this stopped, because I am very, very confident this is not only a huge privacy breach, but this will result in a new, another large data dump, including emails, which is going to allow undesirable parties, not only to have these email-to-user ID matches, but to append the email address to phone numbers, which have been available in previous breaches. I'm quite happy to demonstrate the front-end vulnerability so you can see how this works.

I'm not going to show it in this video, simply because I don't want the video to be, um, I don't want the method to be exploited. But I would be quite happy to demonstrate it if that is necessary. But as you can see, it continues to output more and more and more. I believe this to be quite a dangerous vulnerability, and I would like help in getting this stopped.

This story originally appeared on Ars Technica.

More Great WIRED Stories

- 📩 The latest on tech, science, and more: Get our newsletters!
- A boy, his brain, and a decades-long medical controversy
- How to layer clothes for your next outdoor adventure
- Falcons, Lokis, nerd canons, and why you don’t have to care
- Larry Brilliant has a plan to speed up the pandemic’s end
- Facebook's “Red Team X” hunts bugs beyond its walls

- 👁️ Explore AI like never before with our new database
- 🎮 WIRED Games: Get the latest tips, reviews, and more
- 🎧 Things not sounding right? Check out our favorite wireless headphones, soundbars, and Bluetooth speakers