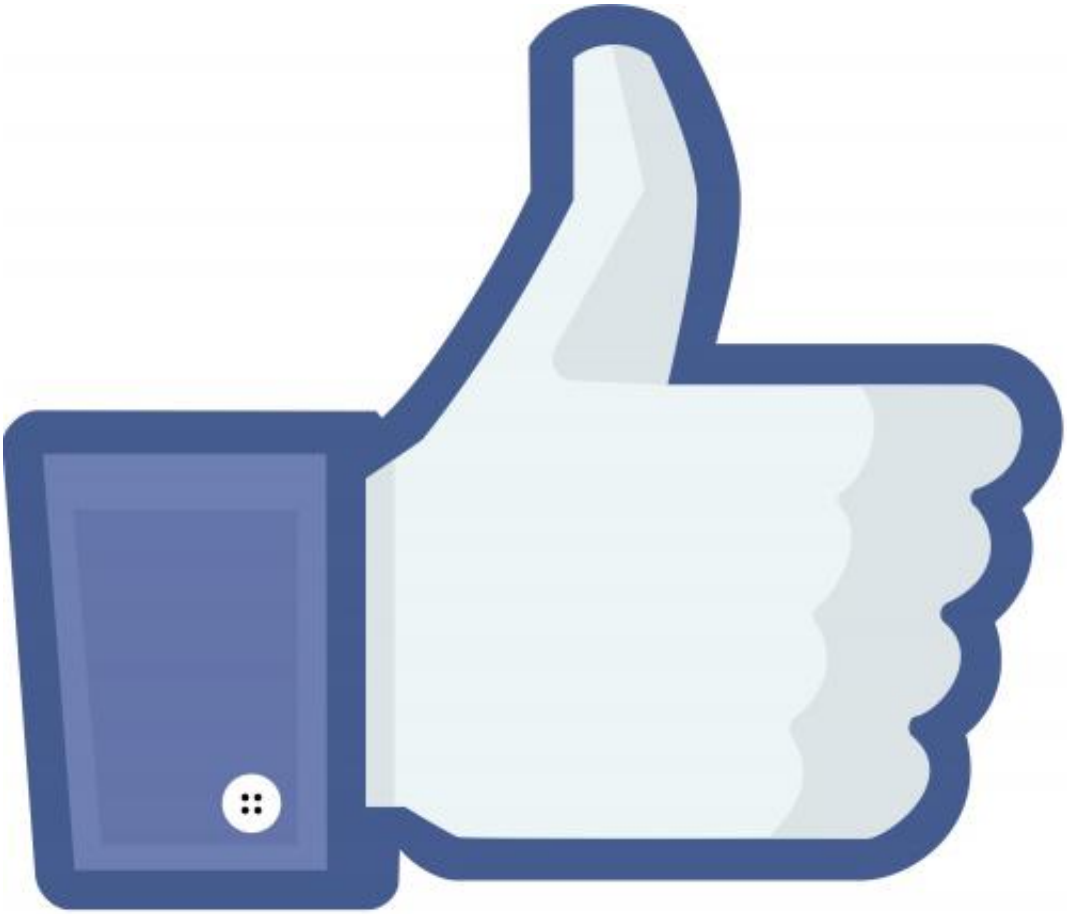
Facebook says bug in Messenger app on Android fixed

June 8 2016, by Nancy Owano



(Tech Xplore)—As many know by now, Facebook recently had a security issue involving Messenger. Outside Facebook, security

researchers said that a bug with the Messenger service would have allowed attackers to change the content of a conversation.

A security team at Check Point found the vulnerability and reported this to Facebook and Facebook fixed it after having run a "thorough investigation," in the words of a Facebook blog posted on Tuesday.

This is how Facebook described the issue: The blog post said that "we recently fixed a straight-forward bug in the way we identified and detected duplicate messages in the Messenger app on Android." Facebook referred to a "misconfiguration with the Messenger app on Android." The blog said "As a result, a sender could write a message and then appear to change its content retroactively."

"We applaud Facebook for such a rapid response, and for working with us to put security first for their users," said Oded Vanunu, head of products vulnerability research at Check Point, according to *The Inquirer*.

Vanunu was also quoted in *Threatpost* by Michael Mimoso: "Facebook was very responsive and took this seriously," Vanunu said. "It's important to understand that this infrastructure is serving hundreds of millions of users. Bringing a code change could be harmful. Facebook managed to close this vulnerability in two weeks."

TechCrunch pointed out that "Only parties in the conversation could exploit the bug—so if you trust your Facebook friends, you probably were not at risk. Since the bug only impacted the Messenger app and in-browser chat on Facebook.com, the authentic conversations would be logged on other versions of Messenger, such as Messenger.com. If someone's chats were manipulated using the bug, he or she would still be able to access the original text in another version of Messenger."

Check Point's research team posted this on its blog on Tuesday:

"The Vulnerability was fully disclosed to the Facebook Security team earlier this month. Facebook immediately responded, and after a joint effort, the vulnerability was patched." Check Point said that Roman Zaikin, security researcher, discovered the vulnerability.

This is how Facebook described the situation on its blog on Tuesday:

"On most clients—including iOS—when duplicate messages are detected, the first message takes precedence and is displayed on both the sender's and receiver's device. However, a misconfiguration with the Messenger app on Android resulted in the last message being displayed instead. As a result, a sender could write a message and then appear to change its content retroactively."

Facebook further stated that "Based on our investigation, this simple misconfiguration in the Messenger app on Android turned out to be a low risk issue and it's already been fixed. We appreciate the whitehat researchers who reported it and helped us create a better experience for all the people who use Messenger."

Kate Conger, a writer covering security at *TechCrunch*, said: "Since the early days of Facebook, the company has run a bug bounty program to encourage security researchers and whitehat hackers to report problems to the company. A Facebook spokesperson told TechCrunch that the program has 'proven incredibly valuable.'"

"Chatting has quickly become a core component in Facebook's product mix," said. Don Reisinger, *PCMag*.

According to Facebook, citing "internal data April 2016," 900 million people are using Messenger every month.

More information: www.facebook.com/notes/faceboo … oid/1310578262289730