Engineer receives $12,500 bounty from Facebook for discovering picture deletion vulnerability

September 3 2013, by Bob Yirka

(Phys.org) —An electronics and communications engineer in India has been awarded a $12,500 bounty by Facebook for the discovery of a picture deleting vulnerability in the social network's Support Dashboard. Arul Kumar details on his blog how he found the vulnerability, how it works and his communications with Facebook regarding the find.

Facebook is serious about its user community following rules about what is posted on user and group pages. For that reason, they have added a

section to the Support Dashboard for users that come across postings or pictures that break the rules so that they can be reported and removed. In looking at how Facebook handled such reports for objectionable photos, Kumar noticed that the code for sending the request could be viewed by the user making the request. He then discovered that the code could be modified as well. Normally, when a report is created it is sent to Facebook, where someone on staff looks at the picture in question and makes a judgment about whether to let it remain or to delete it. If they choose to let it remain, a message is created with a link in it and sent to the owner of the account that holds the photo. That person can then either choose to let the photo remain on their page, or can click the link to have it instantly removed.

Kumar found that he could alter the address to which the message would be sent, which meant he could have it sent to himself, rather than the account holder. Once the message was received, he was then free to click the link to delete the photo. That meant he could delete photos from any account, personal or group—even those posted by others on someone's page, without permission from them or Facebook, and without the knowledge of either. The owner of the page wouldn't know anything had occurred unless they happened to notice a photo missing on their page.

Kumar very carefully followed the rules Facebook has outlined for reporting vulnerabilities (he didn't remove pictures from real user accounts, for example) and was handsomely rewarded for his efforts. He reports that Facebook has subsequently fixed the vulnerability.

https://phys.org/news/2013-09-bounty-facebook-picture-deletion-vulnerability.html