Identify a Facebook user by his phone number despite privacy settings set

MAY 6, 2021

Description

This bug could allow an attacker to identify if a phone number is linked to a Facebook user account and if so what's the id of the user. While adding a phone number in **m.facebook.com** to the attacker Facebook account, the endpoint **m.facebook.com/phoneacquire/** would return the current owner of the phone number despite the privacy settings set by the owner.

Reproduction Steps

1) From the attacker account, go to **https://m.facebook.com/ntdelegatescreen/?params={"saved":true}&path=/contacts/management/**
2) Add a new new phone number that you need to look up if it's linked to a Facebook account
3) A redirect to **https://m.facebook.com/phoneacqwrite/** endpoint should be done. In the attached parameters, there's a parameter called **giver_id** which would be the user id of the Facebook user who has this phone number added to his account.

Impact

This could have been misused to deanonymize/identify a Facebook user account linked to given phone number.

Timeline

Mar 13, 2021—Report Sent
Mar 17, 2021— Acknowledged by Facebook
Apr 7, 2021—Fixed by Facebook
Apr 26, 2021— $9K bounty awarded by Facebook (Including bonus)

UNCATEGORIZED

PREV POST

Account takeover of Instagram accounts due to unrestricted permissions of third-party application's generated tokens

NEXT POST

One-click reflected XSS in www.instagram.com due to unfiltered URI schemes leads to account takeover

SUMMARY

The goal of this blog is to share write-ups about bugs i have found in Facebook and reported to them under the Facebook bug bounty program.

RECENT POSTS

Account Takeover in Canvas Apps served in Comet due to failure in Cross-Window-Message Origin validation

DOM-XSS in Instant Games due to improper verification of supplied URLs

Account takeover of Facebook/Oculus accounts due to First-Party access_token stealing

Multiple bugs chained to takeover Facebook Accounts which uses Gmail.

More secure Facebook Canvas Part 2: More Account Takeovers