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

JANUARY 29, 2023

A malicious actor could steal a first-party access token of the Oculus application which he could use to access the Facebook/Oculus accounts.

This was possible because the Oculus application in Facebook, which was used to login to Oculus using Facebook accounts has **auth.oculus.com/login/** endpoint as a valid redirect_uri. However, Oculus has switched to using Meta Accounts for login. This means that upon visiting **auth.oculus.com/login/**, the endpoint would redirect to auth.meta.com/oidc/ for login using Meta Accounts and then come back to the auth.oculus.com.

We can choose in www.facebook.com OAuth the response_type=token and the token would be passed to the next redirect URL until it reaches again auth.oculus.com. The problem here was that before, auth.oculus.com/login was protecting against token leakage through redirects by having the redirects being made using Javascript , however after the oculus login being changed to Meta accounts and not with Facebook , this protection disappeared and now it directly redirects to the URL initially found in auth.oculus.com/login/?redirect_uri=Redirect_Here. Redirect_Here could be any subdomain of oculus.com and some of them like forums.oculus.com which would redirect to a third party application which can have an open redirect to leak the token (

Setup:

1. Victim is logged-in to Facebook.com
2. Victim is not logged-in to Oculus.com (this is not necessary since we can use a logout CSRF here)

Attack:

1) Login CSRF the victim to his Meta account by redirecting to this page https://auth.meta.com/login/facebook/

2) Open **https://www.facebook.com/v3.1/dialog/oauth?app_id=1517832211847102&redirect_uri=https://auth.oculus.com/login/?redirect_uri=https://forums.oculus.com/openredirect&response_type=token**

3) After the OAuth flow we can notice that the token ended up in https://forums.oculusvr.com/openredirect#access_token=TOKEN

4) Eventually the access_token would be leaked to https://ysamm.com

The open redirect here was not fully disclosed since it’s still not fully fixed.

Timeline

Sep 25, 2022— $44250 bounty awarded by Meta. (Including BountyCon bonuses and bonus for **Highest Impact Report**)

UNCATEGORIZED

‹ PREV POST

Multiple bugs chained to takeover Facebook Accounts which uses Gmail.

NEXT POST ›

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

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.

Search

RECENT POSTS

stealing

Multiple bugs chained to takeover Facebook Accounts which uses Gmail.

More secure Facebook Canvas Part 2: More Account Takeovers