Monday, March 31, 2025 at 1:01 PM

What you submitted

Title
Improper Validation of Current Password During Password Change

Vuln Type
Account Takeover

Product Area
iOS

Description/Impact
While attempting to change my account password in the Instagram app, I noticed a critical issue. Instagram asks users to provide their current password, the new password, and to confirm the new password. However, when I mistakenly entered an incorrect current password (e.g., “ExamplePassword123”) instead of the actual password, Instagram still allowed me to successfully change my password. This indicates that Instagram does not properly validate the current password during the password change process.

This vulnerability could allow unauthorized individuals with temporary or limited access to a user’s device to change the account password without knowing the original password. Consequently, it could lead to unauthorized account access, loss of account control, and compromise user data privacy and security.

Repro Steps
Mobile app version: 374.0.0

See options

Repro Steps
Mobile app version: 374.0.0

Users: Single user logged into their own account

Environment: N/A

Browser: N/A (mobile app)

OS: iOS 18.3.2

1. Open the Instagram app and navigate to account settings.
2. Select “Password and security”.
3. Select “Change password” and then choose an account.
4. Enter an incorrect current password (e.g., “ExamplePassword123”) in the “Current Password” field.
5. Enter the desired new password in the appropriate fields.
6. Tap “Change Password,” and observe that the password change is successfully accepted, despite providing an incorrect current password.

Tuesday, April 1, 2025 at 12:05 AM

Our reply

Hi Javi,

Thank you for your report.

Can you confirm if the incorrect code is similar to the original password ?

Thanks,

Julien

Meta Security

Monday, March 31, 2025 at 1:01 PM

Our reply

Hola,

Gracias por ponerte en contacto con nosotros. Hemos recibido tu denuncia. El número de tu denuncia es 3901110613460812. Te pedimos que nos des un tiempo razonable para revisarla antes de revelar cualquier información sobre ella. Meta se reserva el derecho de publicar tu denuncia. Para obtener más información, como el ámbito de aplicación, falsos positivos habituales y los términos para cerrar las denuncias por considerarlas no válidas, accede a nuestro sitio web: https://bugbounty.meta.com/

Recuerda que si la denuncia está en otro idioma que no sea inglés, por el momento solo podremos responderte en dicho idioma.

Atentamente.

Not Applicable • Thursday, April 3, 2025 at 1:39 AM

Our reply

Thank you for your concern. We are moving away from requiring reauthentication for sensitive actions, since it can cause unnecessary friction for important processes, especially on mobile devices. Instead, we provide robust disavow flows so that, if someone gains access to another person's account, the original account owner can regain control.

Although this issue does not qualify as a part of our bounty program we appreciate your report. We will follow up with you on any security bugs or with any further questions we may have.

Tuesday, April 1, 2025 at 12:15 AM

You replied

Hi Julien,

No, the incorrect code doesn't need to be similar to the original password — you can actually use anything as the current password, even a single character like "a".

Best regards,

Javi

Tuesday, April 1, 2025 at 12:05 AM

Our reply