Submit #565308: Dígitro NGC Explorer 3.44.15 Improper client-side encryption implementation

Title	**Dígitro NGC Explorer 3.44.15 Improper client-side encryption implementation**
Description	Title: NGC Explorer version 3.44.15 Improper encryption implementation leading to plaintext password transmission Software affected: NGC Explorer version 3.44.15 Vendor: Dígitro Tecnologia - https://digitro.com/ Description: The application implements client-side encryption for passwords before sending them to the server. However, the backend also accepts the password in plaintext. This makes the encryption redundant and misleading, weakening the overall security posture. Technical Details: During login, the client encrypts the password and sends it to the server. However, intercepting and modifying the request (e.g., using Burp Suite or similar) to replace the encrypted password with the original plaintext version still results in successful authentication. This suggests that the backend does not enforce encrypted input. Impact: An attacker can bypass the client-side encryption mechanism entirely and authenticate with the application using plaintext credentials. This exposes users to credential interception attacks and undermines the integrity of the authentication process. Evidences of exploitation will be send by e-mail.
User	Anonymous User
Submission	04/24/2025 11:26 PM (17 days ago)
Moderation	05/10/2025 07:30 AM (15 days later)
Status	Accepted
VulDB Entry	308272 [Dígitro NGC Explorer 3.44.15 Password Transmission client-side enforcement of server-side security]
Points	17

Notice

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling