Submit #551172: Demtec, s.r.o Graphlytic 5.0.7 Cross Site Scripting

Title Demtec, s.r.o Graphlytic 5.0.7 Cross Site Scripting

Description Graphytics version 5.0.7 is vulnerable to Stored Cross-Site Scripting (XSS), allowing attackers to execute malicious JavaScript in a victim's browser. This can lead to session hijacking, as the application does not enforce the HttpOnly flag on session cookies, making them accessible to client-side scripts. Exploiting this vulnerability could result in unauthorized access to user sessions and sensitive information.
The issue was tested in the Dockerized version of Graphytics, following the installation guide provided at: "https://graphlytic.com/doc/latest/Install_with_Docker_on_Ubuntu.html"

Steps to Reproduce:

1. Login to the application.
2. Create a new visualization.
3. Click on save.
4. Write any name under 30 charachters.
5. In the description, add the following payload:

```
"><!---->img src=x onerror=alert(document.cookie) >
```

5. Click on Projects / View the list from top left to execute the Stored XSS payload.

Source ⚠ https://github.com/HexC0d3/graphlytic-xss-exploits/blob/main/stored_xss.md

User addy_pwn (UID 77999)

Submission 04/04/2025 10:30 AM (11 days ago)

Moderation 04/14/2025 11:17 PM (11 days later)

Status Accepted

VulDB Entry 304672 [Demtec Graphytics 5.0.7 /visualization description cross site scripting]

Points 20

⚠ 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