



VDB-304672 · CVE-2025-3613

DEMTEC GRAPHYTICS 5.0.7 /VISUALIZATION DESCRIPTION CROSS SITE SCRIPTING

A vulnerability has been found in Demtec Graphytics 5.0.7 and classified as problematic. This vulnerability affects an unknown code of the file */visualization*. The manipulation of the argument `description` with an unknown input leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-79. The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. As an impact it is known to affect integrity.

The advisory is shared for download at github.com. This vulnerability was named CVE-2025-3613. The exploitation appears to be easy. The attack can be initiated remotely. Successful exploitation requires user interaction by the victim. Technical details and also a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1059.007.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The entry VDB-304671 is pretty similar.

Product

Vendor

- Demtec

Name

- Graphytics

Version

- 5.0.7

CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VulDB Vector: 🔒

VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒

CNA CVSS-BT Score: 🔒

CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 4.7

VulDB Meta Temp Score: 4.5

VulDB Base Score: 3.5

VulDB Temp Score: 3.2

VulDB Vector: 🔒

VulDB Reliability: 🔍

Researcher Base Score: 7.1

Researcher Vector: 🔒

CNA Base Score: 3.5

CNA Vector: 🔒

CVSSv2

Base Score	Base Vector	Temp Score	Temp Vector	Reliability
3.5	AV:N/AC:L/Au:N/C:N/I:N/CR:P/RS:M/UA:U	3.2	AV:N/AC:L/Au:N/C:N/I:N/CR:P/RS:M/UA:U	🔍
7.1	AV:N/AC:L/Au:N/C:N/I:N/CR:P/RS:M/UA:U	7.1	AV:N/AC:L/Au:N/C:N/I:N/CR:P/RS:M/UA:U	🔍
3.5	AV:N/AC:L/Au:N/C:N/I:N/CR:P/RS:M/UA:U	3.5	AV:N/AC:L/Au:N/C:N/I:N/CR:P/RS:M/UA:U	🔍

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting





Class: Cross site scripting

CWE: CWE-79 / CWE-94 / CWE-74

CAPEC: 🔒




ATT&CK: 🔒

Local: No
Remote: Yes


Availability: 
Access: Public
Status: Proof-of-Concept
Download: 
Price Prediction: 
Current Price Estimation: 



Threat Intelligence

Interest: 
Active Actors: 
Active APT Groups: 

Countermeasures

Recommended: no mitigation known
Status: 



0-Day Time: 

Timeline

04/14/2025		Advisory disclosed
04/14/2025	+0 days	VulDB entry created
04/15/2025	+1 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2025-3613 ()
scip Labs: <https://www.scip.ch/en/?labs.20161013>
See also: 

Entry

Created: 04/14/2025 11:22 PM
Updated: 04/15/2025 02:10 PM
Changes: 04/14/2025 11:22 PM (56), 04/15/2025 11:36 AM (30), 04/15/2025 02:07 PM (11), 04/15/2025 02:10 PM (3)

Complete: 🔍

Submitter: addy_pwn

Committer: addy_pwn

Cache ID: 5:310:101

Submit

Accepted

- Submit #551172: Demtec, s.r.o Graphlytic 5.0.7 Cross Site Scripting (by addy_pwn)

Discussion



addy_pwn (+1)

upvote

12 hours ago

Dear Team,

I think the severity of this vulnerability should be higher as:

1. This is a Stored XSS that affects the homepage of the application.
2. A low privileged user can store XSS payloads on home page and perform malicious actions.
3. The session cookie does not have 'http-only' flag set that can result in Session Hijacking / Privilege Escalation.

Thanks!