



VDB-304671 · CVE-2025-3612

# DEMTEC GRAPHYTICS 5.0.7 HTTP GET PARAMETER /VISUALIZATION CROSS SITE SCRIPTING

A vulnerability, which was classified as problematic, was found in Demtec Graphytics 5.0.7. This affects an unknown part of the file `/visualization` of the component `HTTP GET Parameter Handler`. The manipulation with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as 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. This is going to have an impact on integrity.

It is possible to read the advisory at [github.com](https://github.com). This vulnerability is uniquely identified as CVE-2025-3612. The exploitability is told to be easy. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. It demands that the victim is doing some kind of user interaction. Technical details and a public exploit are known. The attack technique deployed by this issue is T1059.007 according to MITRE ATT&CK.

The exploit is shared for download at [github.com](https://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.

Entry connected to this vulnerability is available at VDB-304672.

## 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: 4.3

VulDB Meta Temp Score: 4.1

VulDB Base Score: 4.3

VulDB Temp Score: 3.9

VulDB Vector: 🔒

VulDB Reliability: 🔍

CNA Base Score: 4.3

CNA Vector: 🔒

# CVSSv2

CVSSv2	CVSSv3	CVSSv4	CVSSv2	CVSSv3	CVSSv4
4.3	4.3	4.3	4.3	4.3	4.3
3.9	3.9	3.9	3.9	3.9	3.9
4.3	4.3	4.3	4.3	4.3	4.3

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](https://github.com)

Status: Not defined

CVE: CVE-2025-3612 ()

scip Labs: <https://www.scip.ch/en/?labs.20161013>


See also: 

## Entry

Created: 04/14/2025 11:22 PM

Updated: 04/15/2025 11:36 AM

Changes: 04/14/2025 11:22 PM (56), 04/15/2025 11:36 AM (30)

Complete: 

Submitter: 0xc0de

Cache ID: 5:723:101

# Submit

## Accepted

- [Submit #551123: demtec.sk Graphlytics 5.0.7 Cross Site Scripting \(by 0xc0de\)](#)

## Discussion

No comments yet. Languages: en.

Please log in to comment.