VDB-308286 · CVE-2025-4541 · GCVE-100-308286

LMXCMS 1.41 POST REQUEST ZTACTION.CLASS.PHP MANAGEZT SORTID SQL INJECTION

A vulnerability classified as critical has been found in LmxCMS 1.41. Affected is the function `manageZt` of the file *c\admin\ZtAction.class.php* of the component *POST Request Handler*. The manipulation of the argument `sortid` with an unknown input leads to a sql injection vulnerability. CWE is classifying the issue as CWE-89. The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is traded as CVE-2025-4541. The exploitability is told to be easy. It is possible to launch the attack remotely. Technical details and a public exploit are known. This vulnerability is assigned to T1505 by the MITRE ATT&CK project.

The exploit is shared for download 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. By approaching the search of inurl:c\admin\ZtAction.class.php it is possible to find vulnerable targets with Google Hacking.

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

Entries connected to this vulnerability are available at VDB-299944, VDB-300188, VDB-300268 and VDB-300459.

Product

Name

- LmxCMS

Version

- 1.41

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Sql injection
CWE: CWE-89 / CWE-74 / CWE-707
CAPEC: 🔒
ATT&CK: 🔒

Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Google Hack: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

05/10/2025		Advisory disclosed
05/10/2025	+0 days	VulDB entry created
05/10/2025	+0 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2025-4541 (🔒)
GCVE (CVE): GCVE-0-2025-4541
GCVE (VulDB): GCVE-100-308286
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/10/2025 03:50 PM
Changes: 05/10/2025 03:50 PM (57)
Complete: 🔍
Submitter: xiaoyang
Cache ID: 5:F2D:101

Submit

Accepted

- Submit #567191: LmxCMS v1.41 SQL Injection (by xiaoyang)

Discussion

No comments yet. Languages: en.

Please log in to comment.