VDB-354442 · CVE-2026-5252 · GCVE-100-354442

Z-9527 ADMIN 1.0/2.0 MESSAGE CREATE ENDPOINT MESSAGE.JS CROSS SITE SCRIPTING

CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score

3.2 | $0-$5k | 1.61

Summary

A vulnerability was found in z-9527 admin 1.0/2.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file */server/routes/message.js* of the component *Message Create Endpoint*. Executing a manipulation can lead to cross site scripting. This vulnerability is tracked as CVE-2026-5252. The attack can be launched remotely. Moreover, an exploit is present. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability has been found in z-9527 admin 1.0/2.0 and classified as problematic. This vulnerability affects an unknown code of the file */server/routes/message.js* of the component *Message Create Endpoint*. The manipulation 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 available at github.com. This vulnerability was named CVE-2026-5252. 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. This vulnerability is assigned to T1059.007 by the MITRE ATT&CK project.

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 entries VDB-220814, VDB-251849, VDB-275738 and VDB-275743 are pretty similar.

Product

Vendor

- z-9527

Name

- admin

Version

- 1.0
- 2.0

CPE 2.3

- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 3.5
VulDB Meta Temp Score: 3.2

VulDB Base Score: 3.5
VulDB Temp Score: 3.2
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Cross site scripting
CWE: CWE-79 / CWE-94 / CWE-74
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
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

03/31/2026		Advisory disclosed
03/31/2026	+0 days	VulDB entry created
03/31/2026	+0 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5252 (🔒)
GCVE (CVE): GCVE-0-2026-5252
GCVE (VulDB): GCVE-100-354442
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/31/2026 06:16 PM
Changes: 03/31/2026 06:16 PM (56)
Complete: 🔍
Cache ID: 57:F96:179

Submit

Accepted

- Submit #780613: z-9527 admin ≤ commit 72aaf2d Cross Site Scripting (by github.com)

Discussion

No comments yet. Languages: en.

Please log in to comment.