VDB-355408 · CVE-2026-5618 · GCVE-100-355408

KALCADDLE KODBOX UP TO 1.64 SHAREMAKE/SHARECHECK SITEFROM/SITETO SERVER-SIDE REQUEST FORGERY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.1	$0-$5k	2.24-

Summary

A vulnerability was found in kalcaddle kodbox up to 1.64 and classified as critical. This impacts an unknown function of the component *shareMake/shareCheck*. Executing a manipulation of the argument *siteFrom/siteTo* can lead to server-side request forgery. This vulnerability appears as CVE-2026-5618. The attack may be performed from remote. In addition, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in kalcaddle kodbox up to 1.64. It has been declared as critical. This vulnerability affects an unknown code of the component *shareMake/shareCheck*. The manipulation of the argument `siteFrom/siteTo` with an unknown input leads to a server-side request forgery vulnerability. The CWE definition for the vulnerability is CWE-918. The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared for download at vulnplus-note.wetolink.com. This vulnerability was named CVE-2026-5618. The exploitation appears to be difficult. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details and also a public exploit are known.

It is possible to download the exploit at vulnplus-note.wetolink.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.

See VDB-325959, VDB-341665, VDB-346167 and VDB-352424 for similar entries.

Product

Vendor

- kalcaddle

Name

- kodbox

Version

- 1.0
- 1.1
- 1.2
- 1.3
- 1.4
- 1.5
- 1.6
- 1.7
- 1.8
- 1.9
- 1.10
- 1.11
- 1.12
- 1.13

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.6
VulDB Meta Temp Score: 5.1

VulDB Base Score: 5.6
VulDB Temp Score: 5.1
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Server-side request forgery
CWE: CWE-918
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

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/05/2026	+0 days	VulDB entry last update

Sources

Advisory: vulnplus-note.wetolink.com
Status: Not defined

CVE: CVE-2026-5618 (🔒)
GCVE (CVE): GCVE-0-2026-5618
GCVE (VulDB): GCVE-100-355408
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 05:49 PM
Changes: 04/05/2026 05:49 PM (56)
Complete: 🔍
Submitter: vulnplusbot
Cache ID: 52:2F2:179

Submit

Accepted

- Submit #785572: Kodbox 1.64 SSRF (by vulnplusbot)

Discussion

No comments yet. Languages: en.

Please log in to comment.