VDB-356298 · CVE-2026-5842 · ISSUE 431

DECOLUA 9ROUTER UP TO 0.3.47 ADMINISTRATIVE API ENDPOINT /API AUTHORIZATION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
6.6	$0-$5k	1.42-

Summary

A vulnerability described as critical has been identified in decolua 9router up to 0.3.47. This affects an unknown function of the file */api* of the component *Administrative API Endpoint*. The manipulation results in authorization. This vulnerability was named CVE-2026-5842. The attack may be performed from remote. In addition, an exploit is available. Upgrading the affected component is recommended.

Details

A vulnerability was found in decolua 9router up to 0.3.47. It has been classified as critical. Affected is an unknown code block of the file */api* of the component *Administrative API Endpoint*. The manipulation with an unknown input leads to a authorization vulnerability. CWE is classifying the issue as CWE-639. The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data. 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-2026-5842. The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Technical details and a public exploit are known.

The exploit is shared for download at github.com. It is declared as proof-of-concept.

Upgrading to version 0.3.75 eliminates this vulnerability. The upgrade is hosted for download at github.com.

Product

Type

- Router Operating System

Vendor

- decolua

Name

- 9router

Version

- 0.3.0
- 0.3.1
- 0.3.2
- 0.3.3
- 0.3.4
- 0.3.5
- 0.3.6
- 0.3.7
- 0.3.8
- 0.3.9
- 0.3.10
- 0.3.11
- 0.3.12
- 0.3.13
- 0.3.14

Website

- Product: https://github.com/decolua/9router/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 7.3
VulDB Meta Temp Score: 6.6

VulDB Base Score: 7.3
VulDB Temp Score: 6.6
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Authorization
CWE: CWE-639 / CWE-285 / CWE-266
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: Upgrade
Status: 🔍

0-Day Time: 🔒

Upgrade: 9router 0.3.75

Timeline

04/08/2026		Advisory disclosed
04/08/2026	+0 days	VulDB entry created
04/08/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: 431
Status: Confirmed
Confirmation: 🔒

CVE: CVE-2026-5842 (🔒)
GCVE (CVE): GCVE-0-2026-5842
GCVE (VulDB): GCVE-100-356298
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/08/2026 07:48 PM
Changes: 04/08/2026 07:48 PM (61)
Complete: 🔍

Submitter: cyberthoth
Cache ID: 172:A1C:179

Submit

Accepted

- Submit #790003: 9Router Router 0.3.47-0.3.32 Authorization Bypass (by cyberthoth)

Discussion

No comments yet. Languages: en.

Please log in to comment.