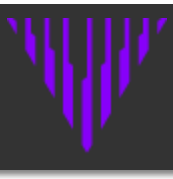

VDB-354132 · CVE-2026-5107 · ID 21098

FRROUTING FRR UP TO 10.5.1 EVPN TYPE-2 ROUTE BGPD/BGP_EVPN.C PROCESS_TYPE2_ROUTE ACCESS CONTROL

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.0	$0-$5k	3.52-

Summary

A vulnerability, which was classified as critical, was found in FRRouting FRR up to 10.5.1. This impacts the function `process_type2_route` of the file *bgpd/bgp_evpn.c* of the component *EVPN Type-2 Route Handler*. The manipulation results in access control. This vulnerability is reported as CVE-2026-5107. The attack can be launched remotely. No exploit exists. It is advisable to implement a patch to correct this issue.

Details

A vulnerability classified as critical has been found in FRRouting FRR up to 10.5.1. Affected is the function `process_type2_route` of the file *bgpd/bgp_evpn.c* of the component *EVPN Type-2 Route Handler*. The manipulation with an unknown input leads to a access control vulnerability. CWE is classifying the issue as CWE-284. The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor. This is going to have an impact on integrity, and availability.

The advisory is shared for download at github.com. This vulnerability is traded as CVE-2026-5107. The exploitability is told to be difficult. It is possible to launch the attack remotely. There are known technical details, but no exploit is available. The MITRE ATT&CK project declares the attack technique as T1068.

Applying the patch 7676cad65114aa23adde583d91d9d29e2debd045 is able to eliminate this problem. The bugfix is ready for download at github.com.

The entries VDB-244512, VDB-330172, VDB-330173 and VDB-330175 are pretty similar.

Product

Vendor

- FRRouting

Name

- FRR

Version

- 10.5.0
- 10.5.1

License

- open-source

Website

- Product: https://github.com/FRRouting/frr/

CPE 2.3

- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 4.2
VulDB Meta Temp Score: 4.0

VulDB Base Score: 4.2
VulDB Temp Score: 4.0
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Access control
CWE: CWE-284 / CWE-266
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Status: Not defined
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

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

Countermeasures

Recommended: Patch
Status: 🔍

0-Day Time: 🔒

Patch: 7676cad65114aa23adde583d91d9d29e2debd045

Timeline

03/29/2026		Advisory disclosed
03/29/2026	+0 days	VulDB entry created
03/29/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: 21098
Status: Confirmed

CVE: CVE-2026-5107 (🔒)
GCVE (CVE): GCVE-0-2026-5107
GCVE (VulDB): GCVE-100-354132
See also: 🔒

Entry

Created: 03/29/2026 08:00 PM
Changes: 03/29/2026 08:00 PM (57)
Complete: 🔍
Submitter: rensiru
Cache ID: 20:10F:179

Submit

Accepted

- Submit #780123: FRRouting FRR 10.5.1 Improper Input Validation (by rensiru)

Discussion

No comments yet. Languages: en.

Please log in to comment.