COMMUNITY CONTENT

Home › Submit › 780123

Submit #780123: FRRouting FRR 10.5.1 Improper Input Validation

Title FRRouting FRR 10.5.1 Improper Input Validation

Description A vulnerability has been identified in FRRouting (FRR) 10.5.1 affecting the processing of EVPN Type-2 (MAC/IP Advertisement) routes within the BGP daemon. The issue is classified as Improper Input Validation (CWE-20) and is located in the function process_type2_route() in bgpd/bgp_evpn.c.

The root cause of the vulnerability is an insufficient consistency check between the NLRI length-related fields psize and ipaddr_len. Although both fields are individually validated against a limited set of acceptable values, the implementation does not enforce that they remain semantically consistent with each other. As a result, a crafted EVPN Type-2 NLRI can satisfy individual validation checks while still carrying an internal field mismatch.

An authenticated remote attacker operating as a legitimate BGP peer with L2VPN EVPN enabled can exploit this condition by advertising a specially crafted EVPN Type-2 route in which psize indicates a larger structure than is actually consumed according to ipaddr_len. Because the parser trusts these fields independently, any remaining bytes in the NLRI may be interpreted as MPLS/VNI label information rather than as malformed route data.

This parsing ambiguity can lead to corruption of EVPN routing information, including incorrect extraction or installation of label-related metadata. In practical VXLAN/EVPN deployments, successful exploitation may result in VNI label poisoning, incorrect tenant-to-VNI mapping, propagation of corrupted EVPN routes, and unintended forwarding behavior across isolation boundaries. Under certain deployment conditions, this may create a risk of traffic leakage, tenant segmentation failure, routing instability, or broader control-plane integrity issues.

The vulnerability does not require local access to the target system, but it does require the attacker to be in a position to establish or control a valid BGP session with EVPN address family support. Given that the attack is performed through crafted control-plane updates, the security impact is especially relevant in environments where BGP peers are not fully trusted or where multi-tenant segmentation depends on the correctness of EVPN route interpretation.

The affected component is bgpd/bgp_evpn.c, specifically the function process_type2_route(). A robust fix should introduce strict cross-validation between psize and ipaddr_len before any label parsing occurs, and the parser should reject any EVPN Type-2 NLRI whose declared structure is not internally consistent.

Source https://github.com/FRRouting/frr/commit/7676cad651144aa23adde583d91d9d29e2debd945

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling

User	rensiru (UID 96440)
Submission	03/14/2026 08:32 AM (16 days ago)
Moderation	03/29/2026 07:55 PM (15 days later)
Status	Published
VulDB entry	[FRRouting FRR up to 10.5.1 EVPN Type-2 Route bgpd/bgp_evpn.c process_type2_route access control]
Points	20