



# CVE-2023-41909

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2023-41909   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2023-09-05 07:15:00 UTC  |
| <b>Updated</b>         | 2023-11-15 05:15:00 UTC  |
| <b>Description</b>     | An issue was discovered in FRRouting FRR through 9.0. bgp_nlri_parse_flowspec in bgpd/bgp_flowspec.c processes malfr |

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                    | Product                      | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Application      | <a href="#">Frrouting</a> | <a href="#">Frrouting</a>    | All     | All    | All     | All      |

## References

| Reference   | Source  | Link  | Tags       |
|---|---------|---|------------|
| [SECURITY] Fedora 37 Update: frr-8.5.3-1.fc37 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |            |
| [SECURITY] [DLA 3573-1] frr security update   | MLIST   | <a href="https://lists.debian.org">lists.debian.org</a>               |            |
| Limit scope by donaldsharp · Pull Request #13222 · FRRouting/frr · GitHub               | MISC    | <a href="https://github.com">github.com</a>                           |            |
| [SECURITY] Fedora 39 Update: frr-8.5.3-1.fc39 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |            |
| [SECURITY] Fedora 38 Update: frr-8.5.3-1.fc38 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |            |
| CVE Program record  | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                         | canonical  |
| NVD vulnerability detail  | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                       | canonical, |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[199835](#) Ubuntu Security Notification for FRR Vulnerabilities (USN-6436-1)

|  |
|--|
| <a href="#">284736</a> Fedora Security Update for frr (FEDORA-2023-ce436d56f8)             |
| <a href="#">284737</a> Fedora Security Update for frr (FEDORA-2023-61abba57d8)             |
| <a href="#">285153</a> Fedora Security Update for frr (FEDORA-2023-514db5339e)             |
| <a href="#">6000142</a> Debian Security Update for frr (DLA 3573-1)                        |
| <a href="#">754897</a> SUSE Enterprise Linux Security Update for frr (SUSE-SU-2023:3709-1) |
| <a href="#">754918</a> SUSE Enterprise Linux Security Update for frr (SUSE-SU-2023:3762-1) |

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)