



CVE-2023-38802

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2023-38802 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-08-29 16:15:00 UTC |
| Updated | 2023-11-15 05:15:00 UTC |
| Description | FRRouting FRR 7.5.1 through 9.0 and Pica8 PICOS 4.3.3.2 allow a remote attacker to cause a denial of service via a crafted |

Risk And Classification

Problem Types: CWE-354

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 11.0 | All | All | All |
| Operating System | Debian | Debian Linux | 12.0 | All | All | All |
| Application | Frrouting | Frrouting | All | All | All | All |
| Operating System | Pica8 | Picos | 4.3.3.2 | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|---|-----------|
| [SECURITY] Fedora 37 Update: frr-8.5.3-1.fc37 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org | |
| [SECURITY] [DLA 3573-1] frr security update | MLIST | lists.debian.org | |
| Debian -- Security Information -- DSA-5495-1 frr | DEBIAN | www.debian.org | |
| [SECURITY] Fedora 39 Update: frr-8.5.3-1.fc39 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org | |
| Grave flaws in BGP Error handling Hacker News | MISC | news.ycombinator.com | |
| [SECURITY] Fedora 38 Update: frr-8.5.3-1.fc38 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org | |
| blog.benjojo.co.uk/post/bgp-path-attributes-grave-error-handling | MISC | blog.benjojo.co.uk | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|---|
| 160921 Oracle Enterprise Linux Security Update for frr (ELSA-2023-5194) |
| 160929 Oracle Enterprise Linux Security Update for frr (ELSA-2023-5219) |
| 242040 Red Hat Update for frr (RHSA-2023:5196) |
| 242041 Red Hat Update for frr (RHSA-2023:5195) |
| 242050 Red Hat Update for frr (RHSA-2023:5194) |
| 242060 Red Hat Update for frr (RHSA-2023:5219) |
| 242107 Red Hat Update for frr (RHSA-2023:5464) |
| 242116 Red Hat Update for frr (RHSA-2023:5457) |
| 242123 Red Hat Update for frr (RHSA-2023:5465) |
| 284736 Fedora Security Update for frr (FEDORA-2023-ce436d56f8) |
| 284737 Fedora Security Update for frr (FEDORA-2023-61abba57d8) |
| 285153 Fedora Security Update for frr (FEDORA-2023-514db5339e) |
| 378922 Alibaba Cloud Linux Security Update for frr (ALINUX3-SA-2023:0120) |
| 6000142 Debian Security Update for frr (DLA 3573-1) |
| 6000208 Debian Security Update for frr (DSA 5495-1) |
| 730909 Palo Alto Networks (PAN-OS) Denial of Service (DoS) Vulnerability in BGP Software (PAN-227523) |
| 754897 SUSE Enterprise Linux Security Update for frr (SUSE-SU-2023:3709-1) |
| 754918 SUSE Enterprise Linux Security Update for frr (SUSE-SU-2023:3762-1) |
| 754933 SUSE Enterprise Linux Security Update for quagga (SUSE-SU-2023:3793-1) |
| 754952 SUSE Enterprise Linux Security Update for quagga (SUSE-SU-2023:3839-1) |
| 754954 SUSE Enterprise Linux Security Update for quagga (SUSE-SU-2023:3836-1) |
| 907313 Common Base Linux Mariner (CBL-Mariner) Security Update for frr (28614-1) |
| 941258 AlmaLinux Security Update for frr (ALSA-2023:5219) |
| 941266 AlmaLinux Security Update for frr (ALSA-2023:5194) |

© [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](#)