



CVE-2022-43681

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-43681
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-03 12:16:00 UTC
Updated	2023-09-19 22:15:00 UTC
Description	An out-of-bounds read exists in the BGP daemon of FRRouting FRR through 8.4. When sending a malformed BGP OPEN message, the daemon will read beyond the end of the message, causing a segmentation fault. This can be exploited to crash the daemon. CVE-2022-43681

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Frrouting	Frrouting	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3573-1] frr security update	MLIST	lists.debian.org	
Debian -- Security Information -- DSA-5495-1 frr	DEBIAN	www.debian.org	
Forescout – Automated Cybersecurity Across Your Digital Terrain	MISC	forescout.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161127 Oracle Enterprise Linux Security Update for frr (ELSA-2023-6434)
242282 Red Hat Update for frr (RHSA-2023:6434)
6000142 Debian Security Update for frr (DLA 3573-1)
6000208 Debian Security Update for frr (DSA 5495-1)

941350 AlmaLinux Security Update for frr (ALSA-2023:6434)

© [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](#)