



FRRouting < 10.5.3 Integer Overflow in OSPF TLV Parser Functions

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

Summary

CVE	CVE-2026-28532
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 21:16:31 UTC
Updated	2026-04-30 21:16:31 UTC
Description	FRRouting before 10.5.3 contains an integer overflow vulnerability in seven OSPF Traffic Engineering and Segment Routin

Risk And Classification

Primary CVSS: v4.0 6 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-125 | CWE-190 | CWE-190 CWE-190: Integer Overflow or Wraparound | CWE-125 CWE-125: Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	6	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/S/
4.0	CNA	CVSS	6	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/S/
3.1	disclosure@vulncheck.com	Primary	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	FRRouting	Frr	affected 10.5.3 semver	Not specified

References

Reference	Source	Link	Tag:
-----------	--------	------	------

github.com/FRRouting/frr/pull/21002	disclosure@vulncheck.com	github.com	
www.vulncheck.com/advisories/frrouting-integer-overflow-in-ospf-tlv-parser-func...	disclosure@vulncheck.com	www.vulncheck.com	
github.com/FRRouting/frr/commit/f098decf02987fbf1c891766c1516ac832adadfd	disclosure@vulncheck.com	github.com	
github.com/FRRouting/frr/releases/tag/frr-10.5.3	disclosure@vulncheck.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

Vendor Comments And Credit

Discovery Credit

CNA: Kazuma Matsumoto, a security researcher at GMO Cybersecurity by IERAE, Inc. (en)

CNA: VulnCheck (en)

There are currently no legacy QID mappings associated with this CVE.

© 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