Traefik: Gateway API TraefikService backend accepts rest@internal, allowing unauthorized exposure of the REST provider despite providers.rest.insecure=false

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-44774
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 17:16:48 UTC
Updated	2026-05-18 17:48:59 UTC
Description	Traefik is an HTTP reverse proxy and load balancer. Prior to 2.11.46, 3.6.17, and 3.7.1, Traefik's Kubernetes Gateway API

Risk And Classification

Primary CVSS: v4.0 6.4 MEDIUM from security-advisories@github.com

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

EPSS: 0.000100000 probability, percentile 0.010880000 (date 2026-05-18)

Problem Types: CWE-284 | CWE-284 CWE-284: Improper Access Control

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	6.4	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:L/S
4.0	CNA	DECLARED	6.4	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:L/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

ntegrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

High

Sub Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Traefik	Traefik	affected < 2.11.46	Not specified
CNA	Traefik	Traefik	affected >= 3.0.0-beta1, < 3.6.17	Not specified
CNA	Traefik	Traefik	affected >= 3.7.0-rc.0, < 3.7.1	Not specified

References

Reference	Source	Link	Tags
github.com/traefik/traefik/releases/tag/v3.7.1	security-advisories@github.com	github.com	
github.com/traefik/traefik/security/advisories/GHSA-96qj-4jj5-wcjc	security-advisories@github.com	github.com	
github.com/traefik/traefik/releases/tag/v2.11.46	security-advisories@github.com	github.com	
github.com/traefik/traefik/releases/tag/v3.6.17	security-advisories@github.com	github.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.

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 registred 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**