



S3 SSE-C Encryption Key Exposed in Plaintext via Config Endpoint (CVE-2025-41118 Pattern)

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

Summary

CVE	CVE-2026-28377
State	PUBLISHED
Assigner	GRAFANA
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 22:16:28 UTC
Updated	2026-03-31 19:00:15 UTC
Description	A vulnerability in Grafana Tempo exposes the S3 SSE-C encryption key in plaintext through the /status/config endpoint, pot

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security@grafana.com

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

EPSS: 0.000100000 probability, percentile 0.011660000 (date 2026-04-01)

Problem Types: CWE-326 | CWE-326 CWE-326 Inadequate Encryption Strength

Version	Source	Type	Score	Severity	Vector
3.1	security@grafana.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Grafana	Tempo	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Grafana	Tempo	affected 2.10.3 semver	OnPrem

References

Reference	Source	Link	Tags
grafana.com/security/security-advisories/cve-2026-28377	security@grafana.com	grafana.com	Vendor Advisory
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 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](#).

CVE.report and Source URL Uptime Status status.cve.report