



RCE on Grafana via sqlExpressions

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

Summary

CVE	CVE-2026-27876
State	PUBLISHED
Assigner	GRAFANA
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 15:16:50 UTC
Updated	2026-03-31 18:36:58 UTC
Description	A chained attack via SQL Expressions and a Grafana Enterprise plugin can lead to a remote arbitrary code execution impact

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from security@grafana.com

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

Problem Types: CWE-94 | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security@grafana.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Grafana	Grafana Enterprise	affected v11.6.0 v11.6.14 semver	OnPrem, Cloud
CNA	Grafana	Grafana Enterprise	affected v12.0.0 v12.1.10 semver	OnPrem, Cloud
CNA	Grafana	Grafana Enterprise	affected v12.2.0 v12.2.8 semver	OnPrem, Cloud
CNA	Grafana	Grafana Enterprise	affected v12.3.0 v12.3.6 semver	OnPrem, Cloud
CNA	Grafana	Grafana Enterprise	affected v12.4.0 v12.4.2 semver	OnPrem, Cloud

References

Reference	Source	Link	Tags
grafana.com/security/security-advisories/cve-2026-27876	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