



CVE-2021-41244

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-41244 |
| State | PUBLIC |
| Assigner | security-advisories@github.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-11-15 20:15:00 UTC |
| Updated | 2022-03-31 16:28:00 UTC |
| Description | Grafana is an open-source platform for monitoring and observability. In affected versions when the fine-grained access con |

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

- [Grafana 8.2.4 released with security fixes | Grafana Labs](#)
- [CVE-2021-41244 Grafana Vulnerability in NetApp Products | NetApp Product Security](#)
- [oss-security - Grafana 8.2.4 released with security fixes](#)
- [Fine-grained access control enables organization admins to create/modify/delete user roles in other organization · Advisory · grafana/grafana](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [502096 Alpine Linux Security Update for grafana](#)
- [690736 Free Berkeley Software Distribution \(FreeBSD\) Security Update for grafana \(99bff2bd-4852-11ec-a828-6c3be5272acd\)](#)
- [700000 CentOS Linux Security Update for grafana](#)

[730289](#) Grafana Enterprise Incorrect Access Control Vulnerability

[752251](#) SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2022:2134-1)

[752995](#) SUSE Enterprise Linux Security Update for grafana (SUSE-SU-2022:4428-1)

© [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](#)