



CVE-2022-29170

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

Summary

CVE	CVE-2022-29170
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-20 16:15:00 UTC
Updated	2022-10-07 15:48:00 UTC
Description	Grafana is an open-source platform for monitoring and observability. In Grafana Enterprise, the Request security feature all

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Release 8.5.3 (2022-05-19) · grafana/grafana · GitHub	MISC	github.cor
Release 7.5.16 (2022-05-19) · grafana/grafana · GitHub	MISC	github.cor
Grafana Enterprise datasource network restrictions bypass via HTTP redirects · Advisory · grafana/grafana · GitHub	CONFIRM	github.cor
CVE-2022-29170 Grafana Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.n
Security: fixes CVE-2022-29170 by xlon · Pull Request #49240 · grafana/grafana · GitHub	MISC	github.cor
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[502306](#) Alpine Linux Security Update for grafana

[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](#)