



CVE-2022-21702

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

Summary

CVE	CVE-2022-21702
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-08 20:15:00 UTC
Updated	2023-11-07 03:43:00 UTC
Description	Grafana is an open-source platform for monitoring and observability. In affected versions an attacker could serve HTML cor

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Grafana	Grafana	All	All	All	All
Application	Grafana	Grafana	2.0.0	beta1	All	All
Application	Grafana	Grafana	2.0.0	beta3	All	All
Application	Netapp	E-series Performance Analyzer	All	All	All	All

References

Reference	Source	Link	Tag
CVE-2022-21702: Grafana proxy XSS · Advisory · grafana/grafana · GitHub	CONFIRM	github.com	
[v7.5.x] Fix for CVE-2022-21702 (#226) · grafana/grafana@2772686 · GitHub	MISC	github.com	
[SECURITY] Fedora 35 Update: grafana-7.5.15-2.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Grafana 7.5.15 and 8.3.5 released with moderate severity security fixes Grafana Labs	MISC	grafana.com	
February 2022 Grafana Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
[SECURITY] Fedora 36 Update: grafana-7.5.15-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 34 Update: grafana-7.5.15-2.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	

[SECURITY] Fedora 36 Update: grafana-7.5.15-2.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 34 Update: grafana-7.5.15-2.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 35 Update: grafana-7.5.15-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [160238](#) Oracle Enterprise Linux Security Update for grafana (ELSA-2022-7519)
- [160278](#) Oracle Enterprise Linux Security Update for grafana (ELSA-2022-8057)
- [240850](#) Red Hat Update for grafana security (RHSA-2022:7519)
- [240902](#) Red Hat Update for grafana security (RHSA-2022:8057)
- [282601](#) Fedora Security Update for grafana (FEDORA-2022-83405f9d5b)
- [282602](#) Fedora Security Update for grafana (FEDORA-2022-9dd03cab55)
- [502305](#) Alpine Linux Security Update for grafana
- [690805](#) Free Berkeley Software Distribution (FreeBSD) Security Update for grafana (cecbc674-8b83-11ec-b369-6c3be5272acd)
- [730423](#) Grafana Multiple Security Vulnerabilities
- [752251](#) SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2022:2134-1)
- [753255](#) SUSE Enterprise Linux Security Update for grafana (SUSE-SU-2022:3765-1)
- [940770](#) AlmaLinux Security Update for grafana (ALSA-2022:7519)
- [940826](#) AlmaLinux Security Update for grafana (ALSA-2022:8057)
- [960182](#) Rocky Linux Security Update for grafana (RLSA-2022:7519)
- [960528](#) Rocky Linux Security Update for grafana (RLSA-2022:8057)

© 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