



CVE-2023-22462

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

Summary

CVE	CVE-2023-22462
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-02 01:15:00 UTC
Updated	2024-02-01 17:08:00 UTC
Description	Grafana is an open-source platform for monitoring and observability. On 2023-01-01 during an internal audit of Grafana, a r

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
Stored XSS in Text plugin · Advisory · grafana/grafana · GitHub	MISC
CVE-2023-22462 Grafana Vulnerability in NetApp Products NetApp Product Security	MISC
Grafana security release: New versions with security fixes for CVE-2023-0594, CVE-2023-0507, and CVE-2023-22462 Grafana Labs	MISC
[v9.3.x] Plugins: Fix plugin query help markdown (#60907) · grafana/grafana@db83d5f · GitHub	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[691080](#) Free Berkeley Software Distribution (FreeBSD) Security Update for grafana (6dccc186-b824-11ed-b695-6c3be5272acd)

[730756](#) Grafana Multiple Stored Cross-Site Scripting (XSS) Vulnerabilities

© [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](#)