



CVE-2021-43798

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

Summary

CVE	CVE-2021-43798
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-07 19:15:00 UTC
Updated	2022-04-12 18:06:00 UTC
Description	Grafana is an open-source platform for monitoring and observability. Grafana versions 8.0.0-beta1 through 8.3.0 (except for

Risk And Classification

EPSS: 0.944380000 probability, percentile 0.999880000 (date 2026-04-01)

CISA KEV: Listed on 2025-10-09; due 2025-10-30; ransomware use Unknown

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	Grafana Labs
Product	Grafana
Name	Grafana Path Traversal Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://grafana.com/blog/2021/12/07/grafana-8.3.1-8.2.7-8.1.8-and-8.0.7-released-with-high-severity-security-fix/ ; https://nvd.nist.gov/vuln/detail/CVE-2021-43798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Grafana	Grafana	All	All	All	All
Application	Grafana	Grafana	8.0.0	beta1	All	All
Application	Grafana	Grafana	8.0.0	beta2	All	All
Application	Grafana	Grafana	8.0.0	beta3	All	All
Application	Grafana	Grafana	8.3.0	All	All	All

References

Reference	Source	Link
Security: Fix directory traversal issue (#42846) · grafana/grafana@c798c0e · GitHub	MISC	github.com
An update on 0day CVE-2021-43798: Grafana directory traversal Grafana Labs	CONFIRM	grafana.com
Grafana Arbitrary File Reading ~ Packet Storm	MISC	packetstormsec
oss-security - CVE-2021-43798 Grafana directory traversal	MLIST	www.openwall.c
December 2021 Grafana Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp
Grafana path traversal · Advisory · grafana/grafana · GitHub	CONFIRM	github.com
oss-security - CVE-2021-43813 and CVE-2021-43815 - Grafana directory traversal for some .md and .csv files	MLIST	www.openwall.c
Grafana 8.3.0 Directory Traversal / Arbitrary File Read ~ Packet Storm	MISC	packetstormsec
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

150439 Grafana Path Traversal Vulnerability (CVE-2021-43798)
502097 Alpine Linux Security Update for grafana
502302 Alpine Linux Security Update for grafana
690738 Free Berkeley Software Distribution (FreeBSD) Security Update for grafana (e33880ed-5802-11ec-8398-6c3be5272acd)
730294 Grafana Path Traversal 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)
755764 SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2024:0487-1)
997073 GO (Go) Security Update for github.com/grafana/grafana (GHSA-8pjt-jj86-j47p)

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

CVE.report and Source URL Uptime Status status.cve.report