



CVE-2021-28146

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-28146
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-22 14:15:00 UTC
Updated	2021-03-26 17:17:00 UTC
Description	The team sync HTTP API in Grafana Enterprise 7.4.x before 7.4.5 has an Incorrect Access Control issue. On Grafana insta

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	Source	Lin
Release notes for Grafana 7.4.5 Grafana Labs	MISC	gra
Grafana 6.7.6, 7.3.10, and 7.4.5 released with important security fixes for Grafana Enterprise Grafana Labs	CONFIRM	gra
Grafana Enterprise Grafana Labs	MISC	gra
oss-security - Grafana 7.4.5, 7.3.10 and 6.7.6 released with security fixes for Grafana Enterprose	CONFIRM	ww
Release notes for Grafana 7.3.10 Grafana Labs	MISC	gra
Release Notes v6.7.x - Releases - Grafana Community	MISC	cor
Grafana Enterprise 6.7.6, 7.3.10 and 7.4.5 Security Update - Security Announcements - Grafana Labs Community Forums	MISC	cor
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501864 Alpine Linux Security Update for grafana
730073 Grafana Enterprise Multiple Security Vulnerabilities
750959 OpenSUSE Security Update for SUSE Manager Client Tools (openSUSE-SU-2021:2675-1)
750960 OpenSUSE Security Update for grafana (openSUSE-SU-2021:2662-1)
750964 OpenSUSE Security Update for grafana (openSUSE-SU-2021:1148-1)
750980 OpenSUSE Security Update for SUSE Manager Client Tools (openSUSE-SU-2021:1162-1)

© [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](#)