



# CVE-2022-21673

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

## Summary

<b>CVE</b>	CVE-2022-21673
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-01-18 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:43:00 UTC
<b>Description</b>	Grafana is an open-source platform for monitoring and observability. In affected versions when a data source has the Forward OAuth Identity Token can allow users to access some data sources · Advisory · grafana/grafana · GitHub

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Grafana</a>	<a href="#">Grafana</a>	All	All	All	All

## References

Reference	Source	Link
Release 8.3.4 (2022-01-17) · grafana/grafana · GitHub	MISC	<a href="#">github.com</a>
[SECURITY] Fedora 35 Update: grafana-7.5.15-2.fc35 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: grafana-7.5.15-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: grafana-7.5.15-2.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
CVE-2022-21673 Grafana Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>
Forward OAuth Identity Token can allow users to access some data sources · Advisory · grafana/grafana · GitHub	CONFIRM	<a href="#">github.com</a>
[SECURITY] Fedora 36 Update: grafana-7.5.15-2.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: grafana-7.5.15-2.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
Release 7.5.13 (2022-01-18) · grafana/grafana · GitHub	MISC	<a href="#">github.com</a>
[SECURITY] Fedora 35 Update: grafana-7.5.15-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>

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)

[502304](#) Alpine Linux Security Update for grafana

[752251](#) SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2022:2134-1)

[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](https://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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)