



CVE-2023-3128

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

Summary

CVE	CVE-2023-3128
State	PUBLIC
Assigner	security@grafana.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-22 21:15:00 UTC
Updated	2023-07-21 19:19:00 UTC
Description	Grafana is validating Azure AD accounts based on the email claim. On Azure AD, the profile email field is not unique and ca

Risk And Classification

Problem Types: CWE-290

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
Authentication bypass / account takeover due to bad implementation of Azure AD OAuth - Advisory · grafana/bugbounty · GitHub	MISC
403 Forbidden	MISC
Grafana authentication bypass using Azure AD OAuth Grafana Labs	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160790](#) Oracle Enterprise Linux Security Update for grafana (ELSA-2023-4030)

[161171](#) Oracle Enterprise Linux Security Update for grafana security and enhancement update (ELSA-2023-6972)

[041700](#) Oracle Enterprise Linux Security Update for grafana (ELSA-2023-4030)

241783 Red Hat Update for grafana (RHSA-2023:4030)
242413 Red Hat Update for grafana (RHSA-2023:6972)
379637 Alibaba Cloud Linux Security Update for grafana security and enhancement update (moderate) (ALINUX3-SA-2024:0038)
691197 Free Berkeley Software Distribution (FreeBSD) Security Update for grafana (fdbe9aec-118b-11ee-908a-6c3be5272acd)
730833 Grafana Authentication Bypass Vulnerability
941170 AlmaLinux Security Update for grafana (ALSA-2023:4030)
941470 AlmaLinux Security Update for grafana (ALSA-2023:6972)
960957 Rocky Linux Security Update for grafana (RLSA-2023:4030)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)