Security Advisory 2023-043

Grafana Authentication Bypass Using Azure AD OAuth

June 29, 2023 — v1.0

TLP:CLEAR

History:

- *29/06/2023 — v1.0 – Initial publication*

Summary

On the 22nd of June, 2023, a critical security vulnerability – CVE-2023-3128 – was identified in Grafana. Grafana was found to be validating Azure Active Directory (AD) accounts based on the email claim. However, on Azure AD, the profile email field is not unique and can be easily altered. This issue can lead to Grafana account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant Azure AD OAuth application [1,2].

Technical Details

Grafana is validating Azure AD accounts based on the email claim. On Azure AD, the profile email field is not unique and can be easily modified. This leads to account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant app [1].

The impact extends to all Grafana deployments that utilise Azure AD OAuth with a multi-tenant Azure application and lack of restrictions on user groups allowed to authenticate [1].

Affected Products

The vulnerability affects all Grafana versions from 6.7.0 onwards.

Recommendations

CERT-EU recommends to upgrade all Grafana deployments. Appropriate patches have been applied to Grafana Cloud. Grafana provide alternative mitigation solution that one can implement [1].

References

[1] https://grafana.com/blog/2023/06/22/grafana-security-release-for-cve-2023-3128/

[2] https://grafana.com/security/security-advisories/cve-2023-3128/