مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Grafana

Tracking #:432317121

Date:25-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Grafana that could potentially be exploited to gain unauthorized access and execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

CVE-2025-3260: Bypass Viewer and Editor Permissions

- **Severity**: High (CVSS 8.3)
- This vulnerability allows users with Viewer or Editor roles to bypass dashboard-specific permissions.
- Users with Viewer roles can view dashboards they lack permissions for. Similarly, those with Editor roles can view, edit, or delete dashboards they lack permissions for. If anonymous authentication is configured, anonymous users can also gain unauthorized access to dashboards, depending on the assigned role.

CVE-2025-2703: DOM XSS Vulnerability

- **Severity**: Medium (CVSS 6.8)
- A DOM XSS vulnerability in Grafana's XY chart plugin allows an attacker with Editor permissions to inject an XSS payload, resulting in arbitrary JavaScript execution.
- Arbitrary JavaScript can execute upon rendering affected panels, bypassing existing Content Security Policies and exposing users to potential exploitation.

CVE-2025-3454: Authorization Bypass in Data Source Proxy API

- **Severity**: Medium (CVSS 5.0)
- An authorization bypass vulnerability in Grafana's data source proxy API allows unauthorized read access by manipulating URL paths.
- Users can gain unauthorized read access to GET endpoints in Prometheus and Alertmanager data sources. Other data sources implementing route-specific permissions and basic authorization may also be vulnerable.

Affected Products:

- Grafana OSS and Grafana Enterprise

Affected Versions

- Various versions of Grafana from 8.x to 11.6.x

Fixed Versions:

- Grafana 11.6.0+security-01
- Grafana 11.5.3+security-01
- Grafana 11.4.3+security-01
- Grafana 11.3.5+security-01
- Grafana 11.2.8+security-01
- Grafana 10.4.17+security-01

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Grafana.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://grafana.com/blog/2025/04/22/grafana-security-release-medium-and-high-severity-fixes-for-cve-2025-3260-cve-2025-2703-cve-2025-3454/?mdm=social&src=x&camp=blog