مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Grafana
Tracking #: 432317510
Date:21-07-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Grafana Labs has released security patches addressing two significant vulnerabilities in its observability platform. These vulnerabilities pose a serious risk to user privacy and system integrity.

TECHNICAL DETAILS:

Vulnerability Details:
1. CVE-2025-6023 – High-Severity XSS via Path Traversal & Open Redirect
- **CVSS Score:** 7.6 (High)
- A client-side **Cross-Site Scripting (XSS)** vulnerability arising from a combination of **path traversal and open redirect** allows attackers to craft malicious dashboard URLs that execute arbitrary JavaScript in a victim's browser
- Attackers send a crafted dashboard link to a user. Upon click, the link redirects to an attacker-controlled page that executes JavaScript in the context of the Grafana session.

2. CVE-2025-6197 – Medium-Severity Open Redirect in Organization Switching
- **CVSS Score:** 4.2 (Medium)
- A redirect issue in the **organization switching** mechanism may allow attackers to redirect authenticated users to malicious domains.
- This flaw can be **chained with CVE-2025-6023** for greater impact in multi-tenant environments.

Affected Versions:
>= Grafana 11.5.0

Fixed Versions:
- Grafana 12.0.2+security-01
- Grafana 11.6.3+security-01
- Grafana 11.5.6+security-01
- Grafana 11.4.6+security-01
- Grafana 11.3.8+security-01

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Grafana Labs.

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/2025/07/17/grafana-security-release-medium-and-high-severity-fixes-for-cve-2025-6197-and-cve-2025-6023/