مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Grafana

Tracking #:432315742

Date:01-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Grafana released security updates to address a Broken Object Level Authorization (BOLA) vulnerability that impacts Grafana.

TECHNICAL DETAILS:

A new Broken Object Level Authorization (BOLA) vulnerability affecting Grafana versions has been discovered. This vulnerability, identified as **CVE-2024-1313** with a **CVSS score of 6.5**, enables low-privileged Grafana users to delete dashboard snapshots from other organizations by utilizing the snapshot's keys.

Affected Versions:

- Grafana versions from 9.5.0 before 9.5.18
- Grafana versions from 10.0.0 before 10.0.13
- Grafana versions from 10.1.0 before 10.1.9
- Grafana versions from 10.2.0 before 10.2.6
- Grafana versions from 10.3.0 before 10.3.5

Fixed Versions:

- Grafana versions 10.4.x, 10.3.5, 10.2.6, 10.1.9 or 9.5.18

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed version 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:

1. https://grafana.com/security/security-advisories/cve-2024-1313/