مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Grafana Plugin SDK

Tracking #:432316319

Date:24-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the Grafana Plugin SDK that could be exploited to gain unauthorized access and obtain sensitive information from affected systems.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2024-8986**
- **CVSS Score:** 9.1 (Critical)
- A critical vulnerability exists in the Grafana Plugin SDK, which could lead to the inadvertent exposure of sensitive information, including repository credentials.
- The Grafana Plugin SDK inadvertently bundles build metadata, including the repository URI, into the compiled binary. When developers use repository URIs containing credentials (e.g., for private dependencies), this information can be extracted from the final plugin binary.
- Successful exploitation of this vulnerability could lead to unauthorized access to private repositories, data exfiltration, and supply chain attacks.

Affected Versions:

- **Grafana Plugin SDK:** All versions up to and including 0.249.0

Fixed Versions:

- **Grafana Plugin SDK** Version 0.250.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://nvd.nist.gov/vuln/detail/CVE-2024-8986