مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Grafana Enterprise

Tracking #:432318050

Date:21-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical privilege-escalation vulnerability in the SCIM provisioning feature of Grafana Enterprise. The flaw could allow a malicious or compromised SCIM client to manipulate user identities and gain unauthorized administrative access.

TECHNICAL DETAILS:

Grafana has released emergency updates addressing a critical privilege-escalation vulnerability (CVE-2025-41115, CVSS 10.0) affecting Grafana Enterprise deployments using the SCIM provisioning feature. The flaw allows a malicious or compromised SCIM client to manipulate user identity fields, potentially enabling impersonation of high-privilege accounts, including the Admin user.

Vulnerability Details

- **CVE-2025-41115**
- Severity: Critical (CVSS 10.0)
- The vulnerability originates from how Grafana Enterprise processes SCIM (System for Cross-domain Identity Management) user identities. The SCIM module allows automated identity lifecycle management; however, an oversight in the user identity-mapping logic enables severe privilege escalation.
- Successful exploitation of this vulnerability can lead to:
    - Full privilege escalation
    - Unauthorized access to admin-level functionalities
    - Identity impersonation
    - Potential compromise of dashboards, data sources, and integrated systems

Affected Versions

- Grafana Enterprise 12.0.0 → 12.2.1

Fixed Versions

- Grafana Enterprise 12.3.0
- Grafana Enterprise 12.2.1
- Grafana Enterprise 12.1.3
- Grafana Enterprise 12.0.6

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released 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/2025/11/19/grafana-enterprise-security-update-critical-severity-security-fix-for-cve-2025-41115/