مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High Severity XSS Vulnerability in Grafana

Tracking #:432317296

Date:22-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity cross-site scripting (XSS) vulnerability in Grafana that could be exploited to execute malicious code on affected systems, potentially leading to session hijacking or full account takeover.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2025-4123
- Severity: High (CVSS 7.6)
- A high severity cross-site scripting (XSS) vulnerability exists in Grafana, allowing attackers to redirect users to malicious websites and execute arbitrary JavaScript code. This vulnerability can be exploited without editor permissions and is effective if anonymous access is enabled. The issue also introduces a risk of full-read SSRF if the Grafana Image Renderer plugin is installed.
- The flaw arises from improper handling of client path traversal and open redirect in custom frontend plugins. This allows attackers to craft URLs that, when visited, execute malicious scripts or redirect users to attacker-controlled sites.
- Exploitation of this vulnerability can lead to:
    - User Redirection: Attackers can redirect users to attacker-controlled sites.
    - Arbitrary Code Execution: Malicious scripts can be executed in the victim's browser.
    - Session Hijacking/Account Takeover: Successful exploitation may result in the compromise of user accounts.
    - Extended SSRF Risk: If the Image Renderer plugin is present, attackers may gain unauthorized access to internal resources.

Affected Versions:

This vulnerability affects **all supported Grafana versions** (**8.0 and later**) including:

- Grafana **12.0**
- Grafana **11.6, 11.5, 11.4, 11.3, 11.2**
- Older, unsupported versions dating back to Grafana **8.0**

Fixed Versions:

- Grafana 12.0.0+security-01
- Grafana 11.6.1+security-01
- Grafana 11.5.4+security-01
- Grafana 11.4.4+security-01
- Grafana 11.3.6+security-01
- Grafana 11.2.9+security-01
- Grafana 10.4.18+security-01

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently 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/2025/05/21/grafana-security-release-high-severity-security-fix-for-cve-2025-4123/