



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in Grafana

Tracking #:432316415

Date:21-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability has been identified in Grafana, an open-source data analytics and visualization platform.

TECHNICAL DETAILS:

A critical security vulnerability has been identified in Grafana, an open-source data analytics and visualization platform. Tracked as **CVE-2024-9264**, this vulnerability has a CVSS score of **9.9**, indicating a severe risk of remote code execution (RCE) through command injection and local file inclusion via an experimental feature known as SQL Expressions. This flaw could potentially allow any user with "Viewer" permissions or higher to execute arbitrary commands on affected systems.

Details of the Vulnerability:

- **Vulnerability ID:** CVE-2024-9264
- **CVSS Score:** 9.9 (Critical)
- **Affected Versions:** Grafana \geq v11.0.0 (all v11.x.y are impacted)
- **Exploitation Conditions:** The vulnerability is exploitable if the DuckDB binary is installed and included in the PATH of the Grafana process environment. DuckDB is not included with Grafana by default, meaning only instances where it is installed and accessible are at risk.

Patched Versions:

- 11.0.5+security-01 (security fix only)
- 11.1.6+security-01 (security fix only)
- 11.2.1+security-01 (security fix only)
- 11.0.6+security-01 (includes latest features and security fix)
- 11.1.7+security-01 (includes latest features and security fix)
- 11.2.2+security-01 (includes latest features and security fix)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends Organizations running affected versions of Grafana should upgrade to one of the patched versions immediately to mitigate the risk.

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/2024/10/17/grafana-security-release-critical-severity-fix-for-cve-2024-9264/>