مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical and High Severity Vulnerabilities in Grafana

Tracking #:432318685

Date:30-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Grafana Labs has released urgent security patches addressing two significant vulnerabilities affecting multiple versions of Grafana.

TECHNICAL DETAILS:

Grafana Labs has released urgent security patches addressing two significant vulnerabilities affecting multiple versions of Grafana. These include a critical Remote Code Execution (RCE) flaw and a high-severity Denial-of-Service (DoS) vulnerability.

- **CVE-2026-27876 (CVSS 9.1 – Critical):** Enables arbitrary file write leading to remote code execution.
- **CVE-2026-27880 (CVSS 7.5 – High):** Allows unauthenticated attackers to crash Grafana instances via memory exhaustion.

Affected Versions

- Grafana v11.6.0 and later (CVE-2026-27876)
- Grafana v12.1.0 and later (CVE-2026-27880)

Patched Versions

- 12.4.2
- 12.3.6
- 12.2.8
- 12.1.10
- 11.6.14

RECOMMENDATIONS:

- **Immediate Actions**
  - Upgrade immediately to one of the patched versions.

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/grafana-security-release-critical-and-high-severity-security-fixes-for-cve-2026-27876-and-cve-2026-27880/