مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in graphql-ruby Gem

Tracking #:432316977

Date:17-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability, tracked as CVE-2025-27407, has been identified in the widely used graphql-ruby gem.

TECHNICAL DETAILS:

A critical vulnerability, tracked as CVE-2025-27407, has been identified in the widely used graphql-ruby gem. This flaw, assigned a CVSS score of 9.1, enables remote code execution (RCE) through maliciously crafted GraphQL schema definitions. With over 136 million downloads, this library's widespread use poses a significant security risk. The vulnerability affects all versions of graphql-ruby prior to the patched releases, making immediate remediation imperative.

Vulnerability Details

- **CVE Identifier:**CVE-2025-27407
- **Severity:** Critical (CVSS Score: **9.1**)
- **Affected Versions:** graphql (RubyGems) > 1.11.5
- **Patched Versions:** 1.11.11, 1.12.25, 1.13.24, 2.0.32, 2.1.15, 2.2.17, 2.3.21, 2.4.13

RECOMMENDATIONS:

The UAE Cyber Security Council recommends Users of graphql-ruby must immediately update 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://github.com/rmosolgo/graphql-ruby/security/advisories/GHSA-q92j-grw3-h492