مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical RCE Vulnerability in OpenCTI Platform

Tracking #:432317250

Date:12-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability has been discovered in the OpenCTI Platform, a widely used open-source threat intelligence management system.

TECHNICAL DETAILS:

A critical remote code execution (RCE) vulnerability has been discovered in the OpenCTI Platform, a widely used open-source threat intelligence management system. It allows malicious users to execute arbitrary commands in the hosting environment, potentially resulting in unauthorized root-level access to infrastructure resources.

Vulnerability Details

- CVE ID: CVE-2025-24977
- CVSS Score: 9.1 (Critical)
- Affected Product: OpenCTI Platform
- Affected Version: 6.4.8
- Patched Version: 6.4.11
- Attack Vector: Remote
- Impact: Remote Code Execution, Privilege Escalation, Data Exfiltration
- Exploit Availability: Public Proof-of-Concepts likely imminent due to ease of abuse

RECOMMENDATIONS:

- Upgrade OpenCTI to patched version or later.

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/OpenCTI-Platform/opencti/security/advisories/GHSA-mf88-g2wq-p7qm