مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Zero-Day Vulnerability in IBM QRadar SIEM

Tracking #:432318084

Date:29-11-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a zero-day vulnerability in IBM QRadar SIEM that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

IBM QRadar SIEM is affected by stored cross-site scripting (XSS) vulnerabilities that could allow authenticated users to inject malicious JavaScript into the web interface.

Vulnerability Details
CVE-2025-36170

- **Severity (CVSS 3.1):** 6.4 (Medium)
- A stored cross-site scripting vulnerability exists in IBM QRadar. This vulnerability allows authenticated user to inject arbitrary JavaScript into the Web UI.
- Successful exploitation of this vulnerability can lead to unauthorized script execution, alteration of UI behavior, and potential disclosure of user credentials.

CVE-2025-36138

- **Severity (CVSS 3.1):** 6.4 (Medium)
- IBM QRadar SIEM contains a stored XSS vulnerability that enables authenticated users to embed malicious JavaScript in the Web UI.
- Successful exploitation of this vulnerability can lead to unauthorized script execution, modification of application functionality, and possible credential disclosure.

Affected Versions

- IBM QRadar SIEM: 7.5 – 7.5.0 UP13 IF02

Fixed Versions

- IBM QRadar SIEM: 7.5.0 – QRadar 7.5.0 UP14 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by IBM.

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://www.ibm.com/support/pages/security-bulletin-ibm-qradar-siem-affected-cross-site-scripting-cve-2025-36170-cve-2025-36138