مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Command Execution Vulnerabilities in IBM QRadar SIEM

Tracking #:432317401

Date:23-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed IBM has released a critical security bulletin addressing three vulnerabilities in its widely deployed QRadar Security Information and Event Management (SIEM) platform.

TECHNICAL DETAILS:

IBM has released a critical security bulletin addressing three vulnerabilities in its widely deployed QRadar Security Information and Event Management (SIEM) platform. These vulnerabilities—CVE-2025-36050, CVE-2025-33121, and CVE-2025-33117—affect versions 7.5 to 7.5.0 UP12 IF01 and range in impact from local information disclosure to remote code execution (RCE). Most notably, CVE-2025-33117 enables command execution via autoupdate abuse, with a CVSS score of 9.1.

Vulnerability Details:

1. CVE-2025-33117 – *Remote Command Execution via Autoupdate Abuse*
   - Severity: Critical (CVSS 9.1)
   - Description: A privileged user can upload a malicious autoupdate package to QRadar. Upon processing, the system executes arbitrary code with elevated privileges.
   - Impact: Full remote code execution, potential for backdoors and data destruction

2. CVE-2025-36050 – *Log Information Disclosure*
   - Severity: Medium (CVSS 6.2)
   - Description: QRadar SIEM stores potentially sensitive information in its log files. A local attacker with filesystem access could read these logs and exfiltrate internal data.
   - Impact: Unauthorized access to credentials, configurations, or internal telemetry.

3. CVE-2025-33121 – *XML External Entity (XXE) Injection*
   - Severity: High (CVSS 7.1)
   - Description: QRadar's XML parsing logic is vulnerable to XXE attacks, allowing remote attackers to send crafted XML data and retrieve sensitive files or cause denial-of-service (DoS) by memory exhaustion.
   - Impact: Information disclosure, memory-based DoS

Affected Products:

- IBM QRadar SIEM 7.5 - 7.5.0 UP12 IF01ProGauge

Fixed Version:

- IBM QRadar SIEM 7.5.0 QRadar 7.5.0 UP12 IF02

RECOMMENDATIONS:

- Upgrade Immediately: Apply the QRadar version 7.5.0 UP12 IF02 update to fully mitigate all three vulnerabilities. No workarounds exist.
- Audit Privileged Users: Review and restrict privileged user access. Ensure only authorized personnel have configuration modification rights.

- Harden Autoupdate Processes: Monitor and log autoupdate activities. Disable automatic update mechanisms if not operationally required.

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/node/7237317