IBM QRadar SIEM Vulnerabilities

Vairav CVE Report

Date: June 23, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Multiple vulnerabilities including **CVE-2025-36050, CVE-2025-33121** and **CVE-2025-33117** have been identified in IBM QRadar SIEM. The most severe vulnerability allows privileged users to modify config files to upload a malicious autoupdate file, leading to arbitrary command execution, with a **CVSS score of 9.1 (Critical)**. If exploited, these vulnerabilities could lead to sensitive data exposure and system compromise.

VULNERABILITY DETAILS

CVE-2025-36050

- **Description:** IBM QRadar SIEM stores potentially sensitive information in log files, which may be readable by local users without proper authorization
- **Impact:** Local attackers can retrieve confidential data such as credentials or system details from logs.
- **CVSS Score:** 6.2 (Medium)

CVE-2025-33121

- **Description:** An XML External Entity (XXE) injection issue in QRadar's XML processing can be triggered by remote, authenticated users, leading to data exfiltration or memory resource exhaustion
- **Impact:** Attackers can access sensitive files or cause denial-of-service by manipulating XML parsers.
- **CVSS Score:** 7.1 (High)

CVE-2025-33117

- **Description:** A serious flaw allows a privileged user to modify configuration files and upload a malicious autoupdate payload, resulting in arbitrary command execution across the system.
- **Impact:** Full system compromise when an attacker successfully deploys a crafted update.
- **CVSS Score:** 9.1 (Critical)

AFFECTED VERSIONS

- **IBM QRadar SIEM** versions 7.5 through 7.5.0 Update Package 12 IF01

EXPLOIT DETAILS

- A privileged attacker leveraging **CVE-2025-33117** could insert persistent backdoors via the autoupdate mechanism.
- Meanwhile, authenticated users could exploit **CVE-2025-33121** to leak data or destabilize memory.
- Finally, **CVE-2025-36050** opens the door to insider threats, as malicious local actors can access sensitive logs.

RECOMMENDED ACTIONS

Patch & Upgrade:

- Upgrade to **IBM QRadar SIEM 7.5.0 UP12 IF02** (Interim Fix 02) or later.

ADDITIONAL SECURITY MEASURES

- **Restrict privileged access:** Limit administrator roles and regularly audit for excessive privileges.
- **Monitor XML intake:** Use IDS/IPS to detect suspicious XML patterns or unexpected XXE payloads targeting QRadar endpoints.
- **Validate autoupdate sources:** Enforce code signing and secure channel validation before accepting updates.
- **Audit logs and configurations:** Regularly search for unexpected configuration changes or local access to sensitive data.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-36050
- https://app.opencve.io/cve/CVE-2025-33121
- https://app.opencve.io/cve/CVE-2025-33117
- https://www.ibm.com/support/pages/node/7237317

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com