Severity

Medium

Analysis Summary

CVE-2022-22345 CVSS:4.8

IBM QRadar 7.3, 7.4, and 7.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.

CVE-2021-38939 CVSS:3.7

IBM QRadar SIEM 7.3, 7.4, and 7.5 stores potentially sensitive information in log files that could be read by an user with access to creating domains.

CVE-2021-38919 CVSS:5.9

IBM QRadar SIEM 7.3, 7.4, and 7.5 in some senarios may reveal authorized service tokens to other QRadar users.

CVE-2021-38878 CVSS:5.9

IBM QRadar 7.3, 7.4, and 7.5 could allow a malicious actor to impersonate an actor due to key exchange without entity authentication.

CVE-2021-38874 CVSS:4.3

IBM QRadar SIEM 7.3, 7.4, and 7.5 allows for users to access information across tenant and domain boundaries in some situations.

CVE-2021-38869 CVSS:4.3

IBM QRadar SIEM 7.3, 7.4, and 7.5 in some situations may not automatically log users out after they exceede their idle timeout.

CVE-2021-29776 CVSS:3.1

IBM QRadar SIEM 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information from another user's dashboard providing the dashboard ID of that user.

Impact

- Cross-Site Scripting
- Information Disclosure
- Security Bypass

Indicators Of Compromise

CVE

- CVE-2022-22345
- CVE-2021-38939
- CVE-2021-38919
- CVE-2021-38878
- CVE-2021-38874
- CVE-2021-38869
- CVE-2021-29776

Affected Vendors

IBM

Affected Products

- IBM QRadar SIEM 7.3.3
- IBM QRadar SIEM 7.4.3
- IBM QRadar SIEM 7.5.0

Remediation

Refer to IBM Security Advisory for patch, upgrade or suggested workaround information.

IBM Security Advisory