TLP: WHITE

# Advisory Alert

**Alert Number:** **AAA20230214** **Date:** **February 14, 2023**

**Document Classification Level** : Public Circulation Permitted | Public

**Information Classification Level** : TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **IBM** | **Critical** | Arbitrary code execution Vulnerability |
| **IBM** | **High** , **Medium** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High** |
| Affected Vulnerability | Arbitrary code execution Vulnerability (CVE-2022-42889, CVE-2022-40674) |
| Description | IBM has released a security update addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to arbitrary code execution.<br>**CVE-2022-42889**- Apache Commons Text could allow a remote attacker to execute arbitrary code on the system, caused by an insecure interpolation defaults flaw. By sending a specially-crafted input, an attacker could exploit this vulnerability to execute arbitrary code on the system.<br>**CVE-2022-40674**-Vulnerability in libexpat could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in the doContent function in xmlparse.c.<br>IBM highly recommends to apply necessary fixes to avoid issues. |
| Affected Products | IBM Db2 Web Query for i version 2.3.0<br>IBM Db2 Web Query for i version 2.4.0<br>IBM QRadar SIEM version 7.4.0 - 7.4.3 Fix Pack 7<br>IBM QRadar SIEM version 7.5.0 - 7.5.0 Update Pack 3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/6955251<br>https://www.ibm.com/support/pages/node/6955057 |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High** , **Medium** |
| Affected Vulnerability | Multiple vulnerabilities (CVE-2022-31160, CVE-2022-41974, CVE-2022-29154, CVE-2022-2625, CVE-2022-2526, CVE-2022-25168, CVE-2022-38177, CVE-2022-38178, CVE-2022-21125, CVE-2022-21127, CVE-2022-21166, CVE-2022-21123, CVE-2021-2163, CVE-2022-34351 ) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to remote code execution, Denial of service, system crash and sensitive information disclosure.<br>IBM recommends to apply necessary fixes to avoid issues. |
| Affected Products | IBM QRadar SIEM version 7.4.0 - 7.4.3 Fix Pack 7<br>IBM QRadar SIEM version 7.5.0 - 7.5.0 Update Pack 3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/6955059<br>https://www.ibm.com/support/pages/node/6955057 |

**Disclaimer**

**The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.**