Advisory Alert

Alert Number: AAA20240725 **Date:** July 25, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37601, CVE-2021-23436, CVE-2021-3757, CVE-2023-42282, CVE-2021-42740, CVE-2021-24033)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar Data Synchronization App for IBM QRadar SIEM. Exploitation of these vulnerabilities may lead to denial of service, arbitrary code execution, and sensitive information disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Data Synchronization App 1.0 - 3.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7161462

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47459, CVE-2022-36402, CVE-2022-38457, CVE-2022-40133, CVE-2022-48743, CVE-2023-5633, CVE-2023-33951, CVE-2023-33952, CVE-2023-52434, CVE-2023-52439, CVE-2023-52450, CVE-2023-52518, CVE-2023-52578, CVE-2023-52707, CVE-2023-52811, CVE-2024-1151, CVE-2024-26581, CVE-2024-26668, CVE-2024-26698, CVE-2024-26704, CVE-2024-26739, CVE-2024-26773, CVE-2024-26808, CVE-2024-26810, CVE-2024-26880, CVE-2024-26908, CVE-2024-26923, CVE-2024-26925, CVE-2024-26929, CVE-2024-26931, CVE-2024-26982, CVE-2024-27016, CVE-2024-27019, CVE-2024-27020, CVE-2024-27065, CVE-2024-27417, CVE-2024-35791, CVE-2024-35897, CVE-2024-35899, CVE-2024-35950, CVE-2024-36025, CVE-2024-36489, CVE-2024-36904, CVE-2024-36924, CVE-2024-36952, CVE-2024-36978, CVE-2024-38596)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to integer overflow, use-after-free, stack overflow, race condition leading to information disclosure. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:4831 • https://access.redhat.com/errata/RHSA-2024:4823

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20919, CVE-2024-20926, CVE-2024-20945, CVE-2023-33850, CVE-2022-37603, CVE-2020-28477, CVE-2022-43441, CVE-2022-25883, CVE-2016-10540, CVE-2024-28863, CVE-2021-23364, CVE-2023-0842, CVE-2022-25881, CVE-2024-29041, CVE-2016-10538, CVE-2018-16487, CVE-2018-3721)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Sensitive information disclosure, Denial of Service, Privilege Escalation, Buffer overflow. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Data Synchronization App 1.0 - 3.1.2 Below Versions of IBM Db2 on Linux and Unix platforms • IBM Db2 10.5.0 - 10.5.11 • IBM Db2 11.1.4 - 11.1.4.7 • IBM Db2 11.5.0 - 11.5.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7161462 • https://www.ibm.com/support/pages/node/7156525

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.