Advisory Alert

Alert Number: AAA20250102 **Date:** January 2, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-41110, CVE-2022-0759, CVE-2024-27281)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in several components which affect IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data. **CVE-2024-41110** - A security vulnerability has been detected in certain versions of Docker Engine, which could allow an attacker to bypass authorization plugins (AuthZ) under specific circumstances. Using a specially-crafted API request, an Engine API client could make the daemon forward the request or response to an authorization plugin without the body. In certain circumstances, the authorization plugin may allow a request which it would have otherwise denied if the body had been forwarded to it. This could lead to unauthorized actions, including privilege escalation. **CVE-2022-0759** - ManageIQ Kubeclient is vulnerable to a man-in-the-middle attack, caused by a flaw when the kubeconfig file does not configure custom CA to verify certs. An attacker could exploit this vulnerability to launch a man-in-the-middle attack and gain access to the communication channel between endpoints to obtain sensitive information or further compromise the system. **CVE-2024-27281** - Ruby RDoc gem could allow a remote attacker to execute arbitrary code on the system, caused by an object injection flaw when parsing .rdoc_options as a YAML file. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data : v3.5 through refresh 10 v4.0 through refresh 9 v4.5 through refresh 3 v4.6 through refresh 6 v4.7 through refresh 4 v4.8 through refresh 6 v5.0 through refresh 2 v5.0 through refresh 3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7180105

Affected Product	**IBM**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20952, CVE-2024-20918, CVE-2024-2961, CVE-2024-33599, CVE-2023-41993, CVE-2024-4068, CVE-2023-6597, CVE-2024-37890, CVE-2024-6345, CVE-2024-2398, CVE-2024-39338, CVE-2024-29857, CVE-2024-37370, CVE-2024-37371, CVE-2024-45296, CVE-2024-6119, CVE-2024-45491, CVE-2024-45590, CVE-2024-41123, CVE-2024-41946, CVE-2024-47220, CVE-2022-24795, CVE-2022-31163, CVE-2021-32740, CVE-2021-41186, CVE-2023-45288, CVE-2024-47554, CVE-2023-39325, CVE-2023-45283, CVE-2024-24786, CVE-2024-0406, CVE-2024-33883)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in several components which affect IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data. Exploitation of these vulnerabilities may lead to Denial of Service, Arbitrary Code Execution, Server-Side Request Forgery, Security Restrictions Bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data : v3.5 through refresh 10 v4.0 through refresh 9 v4.5 through refresh 3 v4.6 through refresh 6 v4.7 through refresh 4 v4.8 through refresh 6 v5.0 through refresh 2 v5.0 through refresh 3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7180105

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.