# Advisory Alert

**Alert Number:** AAA20251007 **Date:** October 7, 2025

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **IBM** | **Critical** | Multiple Vulnerabilities |
| **QNAP** | **High**, **Medium** | Multiple Vulnerabilities |
| **Zabbix** | **High**, **Medium**, **Low** | Multiple Vulnerabilities |
| **IBM** | **High**, **Medium**, **Low** | Multiple Vulnerabilities |
| **Red Hat** | **Medium** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-45337, CVE-2025-6965) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2025-6965** - There exists a vulnerability in SQLite versions before 3.50.2 where the number of aggregate terms could exceed the number of columns available. This could lead to a memory corruption issue.<br>**CVE-2024-45337** - Applications and libraries which misuse connection.serverAuthenticate (via callback field ServerConfig.PublicKeyCallback) may be susceptible to an authorization bypass.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | AIX versions 7.2 and 7.3<br>VIOS versions 3.1 and 4.1<br>IBM DB2 Data Management Console version 3.1.13<br>IBM DB2 Data Management Console on CPD versions 4.8.8, CPD 5.0.0 - CPD 5.1.3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7247272<br>• https://www.ibm.com/support/pages/node/7247188 |

| | |
|---|---|
| Affected Product | **QNAP** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-33034, CVE-2025-33039, CVE-2025-33040, CVE-2025-44006, CVE-2025-44007, CVE-2025-44008, CVE-2025-44009, CVE-2025-44010, CVE-2025-44011, CVE-2025-44012, CVE-2025-44014, CVE-2025-47210, CVE-2025-47211, CVE-2025-47212, CVE-2025-47213, CVE-2025-47214, CVE-2025-48726, CVE-2025-48727, CVE-2025-48728, CVE-2025-48729, CVE-2025-48730, CVE-2025-52424, CVE-2025-52427, CVE-2025-52428, CVE-2025-52429, CVE-2025-52432, CVE-2025-52433, CVE-2025-52853, CVE-2025-52854, CVE-2025-52855, CVE-2025-52857, CVE-2025-52858, CVE-2025-52859, CVE-2025-52860, CVE-2025-52862, CVE-2025-52866, CVE-2025-52867, CVE-2025-53406, CVE-2025-53407, CVE-2025-53595, CVE-2025-54153, CVE-2025-54154, CVE-2025-57714) |
| Description | QNAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Path Traversal, denial-of-service, memory corruption, unauthorized code or commands execution.<br>QNAP advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | QNAP Authenticator 1.3.x versions prior to 1.3.1.1227<br>Qsync Central 4.x versions prior to 5.0.0.1 (2025/07/09)<br>Qsync Central 5.0.0 versions prior to 5.0.0.2 (2025/07/31)<br>QTS 5.2.x versions prior to 5.2.6.3195 build 20250715<br>QuTS hero h5.2.x versions prior to h5.2.6.3195 build 20250715<br>NetBak Replicator 4.5.x versions prior to 4.5.15.0807 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.qnap.com/en/security-advisory/qsa-25-30<br>• https://www.qnap.com/en/security-advisory/qsa-25-34<br>• https://www.qnap.com/en/security-advisory/qsa-25-35<br>• https://www.qnap.com/en/security-advisory/qsa-25-36<br>• https://www.qnap.com/en/security-advisory/qsa-25-39 |

| | |
|---|---|
| Affected Product | **Zabbix** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-49641, CVE-2025-27231, CVE-2025-27237, CVE-2025-27236) |
| Description | Zabbix 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, Local Privilege Escalation and perform unauthorized actions.<br>Zabbix advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Zabbix Frontend, Agent and Agent2 versions:<br>• 6.0.0 - 6.0.40<br>• 7.0.0 - 7.0.17<br>• 7.2.0 - 7.2.11<br>• 7.4.0 - 7.4.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://support.zabbix.com/browse/ZBX-27063<br>• https://support.zabbix.com/browse/ZBX-27062<br>• https://support.zabbix.com/browse/ZBX-27061<br>• https://support.zabbix.com/browse/ZBX-27060 |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-3651, CVE-2023-24532, CVE-2022-41724, CVE-2022-41725, CVE-2022-41723, CVE-2024-26973, CVE-2024-26907, CVE-2023-52477, CVE-2024-26901, CVE-2024-26645, CVE-2023-52492, CVE-2023-52869, CVE-2023-52560, CVE-2023-52683, CVE-2023-52622, CVE-2023-52672, CVE-2024-26934, CVE-2024-26964, CVE-2022-48669) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service and memory leak.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | IBM DB2 Data Management Console version 3.1.13<br>IBM DB2 Data Management Console on CPD versions 4.8.8, CPD 5.0.0 - CPD 5.1.3<br>IBM DB2 Data Management Console all versions<br>IBM Storage Scale System versions 6.1.9.0 - 6.1.9.7 and 6.2.0.0 - 6.2.3.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7247188<br>• https://www.ibm.com/support/pages/node/7247086<br>• https://www.ibm.com/support/pages/node/7246320<br>• https://www.ibm.com/support/pages/node/7246319 |

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-50301, CVE-2025-38351, CVE-2025-39761) |
| Description | Red Hat has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2024-50301** - security/keys: fix slab-out-of-bounds in key_task_permission.<br>**CVE-2025-38351** - KVM: x86/hyper-v: Skip non-canonical addresses during PV TLB flush.<br>**CVE-2025-39761** - wifi: ath12k: Decrement TID on RX peer frag setup error handling.<br>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Red Hat Enterprise Linux for x86_64 9 x86_64<br>Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64<br>Red Hat Enterprise Linux Server - AUS 9.6 x86_64<br>Red Hat Enterprise Linux for IBM z Systems 9 s390x<br>Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x<br>Red Hat Enterprise Linux for Power, little endian 9 ppc64le<br>Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le<br>Red Hat Enterprise Linux for ARM 64 9 aarch64<br>Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64<br>Red Hat CodeReady Linux Builder for x86_64 9 x86_64<br>Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le<br>Red Hat CodeReady Linux Builder for ARM 64 9 aarch64<br>Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x<br>Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64<br>Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le<br>Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x<br>Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64<br>Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64<br>Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/errata/RHSA-2025:17377 |

**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.**