# Advisory Alert

**Alert Number:** AAA20251028 **Date:** October 28, 2025

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Red Hat** | **High**, Medium | Multiple Vulnerabilities |
| **IBM** | **High**, Medium, Low | Multiple Vulnerabilities |
| **Apache Tomcat** | **High**, Low | Multiple Vulnerabilities |
| **Dell** | Medium | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **High**, Medium |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-6021, CVE-2025-49794, CVE-2025-49795, CVE-2025-49796, CVE-2025-59375, CVE-2025-38556, CVE-2025-38571, CVE-2025-38614, CVE-2025-39718, CVE-2025-39682, CVE-2025-39751, CVE-2023-53373) |
| Description | Red Hat has released security updates addressing multiple vulnerabilities that exist in their products.<br>These vulnerabilities could be exploited by malicious users in order to conduct Denial of Service (DoS), Memory Modification, Unauthorized Command Execution and Bypass Protection Mechanism.<br>Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Red Hat JBoss Core Services Text-Only Advisories x86_64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le<br>Red Hat Enterprise Linux Server - AUS 9.4 x86_64<br>Red Hat Enterprise Linux for x86_64 8 x86_64<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64<br>Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64<br>Red Hat Enterprise Linux for Power, little endian 8 ppc64le<br>Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le<br>Red Hat Enterprise Linux for IBM z Systems 8 s390x<br>Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x<br>Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x<br>Red Hat Enterprise Linux for ARM 64 8 aarch64<br>Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64<br>Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64<br>Red Hat CodeReady Linux Builder for x86_64 8 x86_64<br>Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64<br>Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le<br>Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le<br>Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x<br>Red Hat CodeReady Linux Builder for ARM 64 8 aarch64<br>Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://access.redhat.com/errata/RHSA-2025:19020<br>• https://access.redhat.com/errata/RHSA-2025:19104<br>• https://access.redhat.com/errata/RHSA-2025:19102 |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, Medium, Low |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-33126, CVE-2025-33131, CVE-2025-33133, CVE-2025-33132, CVE-2025-38211, CVE-2025-38332, CVE-2025-38464, CVE-2025-38477, CVE-2025-48989, CVE-2025-50059, CVE-2025-50106, CVE-2025-30749, CVE-2025-30761, CVE-2025-30754, CVE-2025-54389, CVE-2025-8713, CVE-2025-8714, CVE-2025-8715, CVE-2024-47081, CVE-2025-8058, CVE-2022-26336, CVE-2024-47554, CVE-2025-40909, CVE-2025-36007, CVE-2025-36170, CVE-2025-36138) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products.<br>These vulnerabilities could be exploited by malicious users in order to conduct Incorrect Privilege Assignment, Cross-site Scripting, Buffer Overflow, Improper Access Control, and Improper Input Validation.<br>IBM advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | IBM DB2 High Performance Unload 6.1.0.3<br>IBM DB2 High Performance Unload 5.1.0.1<br>IBM DB2 High Performance Unload 6.1.0.2<br>IBM DB2 High Performance Unload 6.5<br>IBM DB2 High Performance Unload 6.5.0.0 IF1<br>IBM DB2 High Performance Unload 6.1.0.1<br>IBM DB2 High Performance Unload 6.1<br>IBM DB2 High Performance Unload 5.1<br>IBM QRadar SIEM 7.5 - 7.5.0 UP13 IF02 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7249336<br>• https://www.ibm.com/support/pages/node/7249276<br>• https://www.ibm.com/support/pages/node/7249277<br>• https://www.ibm.com/support/pages/node/7249278 |

| | |
|---|---|
| Affected Product | **Apache Tomcat** |
| Severity | **High**, Low |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-61795, CVE-2025-55754, CVE-2025-55752) |
| Description | The ASF has released security updates addressing multiple vulnerabilities that exist in their Apache Tomcat.<br>These vulnerabilities could be exploited by malicious users in order to conduct Denial of Service (DoS), Remote Code Execution and Console Manipulation.<br>The ASF advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Apache Tomcat version 11.0.0-M1 to 11.0.11<br>Apache Tomcat version 10.1.0-M1 to 10.1.46<br>Apache Tomcat version 9.0.0.M1 to 9.0.109 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://tomcat.apache.org/security-11.html<br>• https://tomcat.apache.org/security-10.html<br>• https://tomcat.apache.org/security-9.html |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025- 46602, CVE-2024-36350, CVE-2024-36357) |
| Description | Dell has released security updates addressing multiple vulnerabilities that exist in their products.<br>These vulnerabilities could be exploited by malicious users in order to conduct Sensitive Information Leakage.<br>Dell advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Dell SupportAssist OS Recovery Versions prior to 5.5.15.0<br>Alienware Aurora R15 AMD Versions prior to 1.19.0<br>Alienware Aurora Ryzen Edition R14 Versions prior to 2.24.0<br>Alienware m15 R7 AMD Versions prior to 1.23.0<br>Alienware m15 Ryzen Edition R5 Versions prior to 1.28.0<br>Alienware m16 R1 AMD Versions prior to 1.18.0<br>Alienware m17 R5 AMD Versions prior to 1.23.0<br>Alienware m18 Versions prior to 1.18.0<br>Dell G15 5515 Versions prior to 1.27.0<br>Dell G15 5525 Versions prior to 1.23.0<br>Dell G15 5535 Versions prior to 1.14.0<br>Inspiron 14 5425 Versions prior to 1.23.0<br>Inspiron 14 5435 Versions prior to 1.17.0<br>Inspiron 14 5445 Versions prior to 1.11.0<br>Inspiron 14 7425 2-in-1 Versions prior to 1.23.0<br>Inspiron 14 7435 2-in-1 Versions prior to 1.17.0<br>Inspiron 14 7445 2-in-1 Versions prior to 1.11.0<br>Inspiron 15 3525 Versions prior to 1.30.0<br>Inspiron 15 3535 Versions prior to 1.23.0<br>Inspiron 16 5625 Versions prior to 1.23.0<br>Inspiron 16 5635 Versions prior to 1.17.0<br>Inspiron 16 5645 Versions prior to 1.13.0<br>Inspiron 16 7635 2-in-1 Versions prior to 1.17.0<br>Inspiron 24 5415 All-in-One Versions prior to 1.28.0<br>Inspiron 5415 Versions prior to 1.29.0<br>Inspiron 5515 Versions prior to 1.29.0<br>Inspiron 7415 2-in-1 Versions prior to 1.29.0<br>Precision 7875 Tower Versions prior to 01.13.00<br>Vostro 14 3425 Versions prior to 1.30.0<br>Vostro 14 3435 Versions prior to 1.23.0<br>Vostro 15 3525 Versions prior to 1.30.0<br>Vostro 15 3535 Versions prior to 1.23.0<br>Vostro 16 5635 Versions prior to 1.17.0<br>Vostro 5415 Versions prior to 1.29.0<br>Vostro 5515 Versions prior to 1.29.0<br>Vostro 5625 Versions prior to 1.23.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.dell.com/support/kbdoc/en-us/000382443/dsa-2025-403<br>• https://www.dell.com/support/kbdoc/en-us/000312039/dsa-2025-189 |

**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.**