# Advisory Alert

**Alert Number:** AAA20260522 **Date:** May 22, 2026

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Dell** | **Critical** | Use of Hard-Coded Credentials Vulnerability |
| **Red Hat** | **High** | Multiple Vulnerabilities |
| **IBM** | **High**, Medium | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **Critical** |
| Affected Vulnerability | Use of Hard-Coded Credentials Vulnerability (CVE-2026-40710) |
| Description | Dell has released a security update addressing multiple vulnerabilities that exist in their products.<br><br>**CVE-2026-40710**: Dell Container Storage Modules, versions Operator 1.6.0 through 1.16.3 and Helm Charts 1.11.0 through 1.16.3, contain a Use of Hard-coded Credentials vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure. This vulnerability is considered critical as it exposes default authentication credentials in public source code, enabling unauthorized access to sensitive system components.<br><br>Dell advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Dell Container Storage Modules CSM Operator versions 1.6.0 through 1.16.3<br>Dell Container Storage Modules CSM Helm Charts versions 1.11.0 through 1.16.3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.dell.com/support/kbdoc/en-us/000467149/dsa-2026-234-security-update-for-dell-container-storage-modules-hard-coded-credentials-vulnerability |

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-46300, CVE-2026-46333, CVE-2026-31532) |
| Description | Red Hat has released security updates addressing multiple vulnerabilities that exist in their products.<br><br>**CVE-2026-46300**: A flaw was found in the Linux kernel's XFRM ESP-in-TCP subsystem. Unsafe in-place cryptographic processing allows a low-privileged local attacker to write arbitrary bytes into the page cache of read-only files, including sensitive system files. An attacker can exploit this to overwrite privileged binaries and gain root privileges.<br><br>**CVE-2026-46333**: A vulnerability was found in the Linux kernel that allows an unprivileged local user to read sensitive files normally restricted to the root user. The flaw occurs during process exit, where a brief window allows an attacker to intercept file access from a privileged process before it fully terminates. Successful exploitation may lead to the disclosure of sensitive data such as SSH host private keys or /etc/shadow contents.<br><br>**CVE-2026-31532**: A flaw was found in the Linux kernel's Controller Area Network (CAN) raw socket implementation. A use-after-free vulnerability can occur due to a timing window during the unregistration of CAN receive filters, allowing a freed memory region to be accessed. This could lead to system instability or a denial of service (DoS).<br><br>Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64<br>Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x<br>Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le<br>Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64<br>Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64<br>Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64<br>Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x<br>Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x<br>Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le<br>Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le<br>Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64<br>Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64<br>Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.4 and 8.6 x86_64<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64<br>Red Hat Enterprise Linux Server - AUS 8.4 and 8.6 x86_64<br>Red Hat Enterprise Linux Server - TUS 8.6 x86_64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://access.redhat.com/errata/RHSA-2026:20299<br>• https://access.redhat.com/errata/RHSA-2026:20130<br>• https://access.redhat.com/errata/RHSA-2026:20051 |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-1718, CVE-2025-13755, CVE-2026-6053, CVE-2026-6052, CVE-2026-6051, CVE-2026-6938) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems.<br>IBM advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | DB2 versions:<br>• 11.5.0 to 11.5.9<br>• 12.1.0 to 12.1.4 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7273555<br>• https://www.ibm.com/support/pages/node/7273554<br>• https://www.ibm.com/support/pages/node/7273556<br>• https://www.ibm.com/support/pages/node/7273557<br>• https://www.ibm.com/support/pages/node/7273558<br>• https://www.ibm.com/support/pages/node/7273559 |

**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.**