Advisory Alert

Alert Number: AAA20260811 **Date:** August 11, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-67271, CVE-2026-70415, CVE-2026-67262)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-67271:** Dell PowerStore SDNAS, contains an Out-of-bounds Write vulnerability in the SMB/CIFS. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Denial of service and Remote execution. This is a Critical vulnerability as a remote user could send a specially crafted SMB packet and cause a crash, that is persistent in case automatic restarts are enabled. **CVE-2026-70415:** Dell PowerStore SDNAS contains a Buffer Copy without Checking Size of Input vulnerability in the NFS/RPC. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Command execution and Denial of service. **CVE-2026-67262:** Dell PowerStore contains a Missing Authorization vulnerability. An attacker with access to a mapped host could exploit this vulnerability to read from or write to LUNs that the host is not authorized to access, bypassing per-initiator LUN access controls and leading to protection mechanism bypass. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Versions prior to 5.0.0.2-2761110 • PowerStore 500T • PowerStore 1000T • PowerStore 1200T • PowerStore 3000T • PowerStore 3200Q • PowerStore 3200T • PowerStore 5000T • PowerStore 5200Q • PowerStore 5200T • PowerStore 7000T • PowerStore 9000T • PowerStore 9200T
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000497829/dsa-2026-330-dell-powerstore-t-security-update-for-multiple-vulnerabilities

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-29063, CVE-2026-8633, CVE-2025-62718, CVE-2026-41293, CVE-2026-43512, CVE-2026-43515, CVE-2026-40974, CVE-2026-29145, CVE-2021-24032, CVE-2026-2332, CVE-2026-1525, CVE-2026-33228)
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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Data System - Versions 11.3.0.2-IF1 IBM Db2 Developer Extension - Versions 1.1.1 IBM Storage Protect for Virtual Environments: DP for Hyper-V - Versions 8.1.0.0 - 8.2.1.0 IBM Storage Protect for Virtual Environments: DP for VMware - Versions 8.1.0.0 - 8.2.1.0 IBM Storage Protect Client - Versions 8.1.0.0 - 8.2.1.0 IBM Storage Protect Operations Center - Version 8.1, 8.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7283112 • https://www.ibm.com/support/pages/node/7283130 • https://www.ibm.com/support/pages/node/7283131 • https://www.ibm.com/support/pages/node/7283136 • https://www.ibm.com/support/pages/node/7283138 • https://www.ibm.com/support/pages/node/7283061 • https://www.ibm.com/support/pages/node/7282670 • https://www.ibm.com/support/pages/node/7282671 • https://www.ibm.com/support/pages/node/7282685

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31787, CVE-2026-43112, CVE-2026-46054, CVE-2025-10263, CVE-2026-52923, CVE-2026-53059, CVE-2025-71131, CVE-2026-52976, CVE-2026-64496)
Description	Red Hat 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. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Long Life 8.8 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.6 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.6 s390x Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:52649 • https://access.redhat.com/errata/RHSA-2026:52667 • https://access.redhat.com/errata/RHSA-2026:52765

Vendor	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-32657, CVE-2025-68276, CVE-2026-70412, CVE-2025-29088, CVE-2026-59914, CVE-2026-46731, CVE-2026-59916, CVE-2026-59917, CVE-2025-59603)
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000497857/dsa-2026-220-security-update-for-dell-product-vulnerability • https://www.dell.com/support/kbdoc/en-us/000497884/dsa-2026-349-security-update-for-dell-idrac10-vulnerability • https://www.dell.com/support/kbdoc/en-us/000497902/dsa-2026-348-security-update-for-dell-idrac9-and-idrac10-vulnerability • https://www.dell.com/support/kbdoc/en-us/000497919/dsa-2026-347-security-update-for-dell-idrac9-and-idrac10-vulnerability • https://www.dell.com/support/kbdoc/en-us/000490038/dsa-2026-320-security-updates-for-dell-display-and-peripheral-manager-ddpm-windows-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000480882/dsa-2026-294-security-update-for-dell-client-platform-for-a-qualcomm-mipi-camera-driver-vulnerability

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security Verify Access - Version 10.0 - 10.0.9.2 IBM Verify Identity Access - Version 11.0 - 11.0.3 IBM Verify Identity Access Container - Versions 11.0 - 11.0.3 IBM Security Verify Access Container - Versions 10.0 - 10.0.9.2 IBM Storage Scale Versions: • 5.2.0.0 - 5.2.3.8 • 6.0.0.0 - 6.0.1.0 IBM Storage Protect for Space Management - Versions 8.1.0.0 - 8.2.1.0 IBM Cloud Pak for Data System - Versions 11.3.0.2-IF1 IBM Db2 Developer Extension - Versions 1.1.1 IBM Storage Protect for Virtual Environments: DP for Hyper-V - Versions 8.1.0.0 - 8.2.1.0 IBM Storage Protect for Virtual Environments: DP for VMware - Versions 8.1.0.0 - 8.2.1.0 IBM Storage Protect Client - Versions 8.1.0.0 - 8.2.1.0 IBM Storage Protect Operations Center - Version 8.1, 8.2 IBM Security QRadar Log Management AQL Plugin - Versions 1.0.0 - 1.1.7 QRadar AI Assistant - Versions 1.0.0 - 2.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/

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.