Advisory Alert

Alert Number: AAA20260210 **Date:** February 10, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
NetApp	**Medium**	Uncontrolled Resource Consumption Vulnerability
Synology	**Medium**	Information Disclosure Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell 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 system. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.

Affected Products	• Dell Avamar Data Store Gen4T and Gen5A on SUSE Linux Enterprise 12 SP5 Versions 19.12, 19.10 – SP1, 19.10 and 19.9
	• Dell Avamar Virtual Edition on SUSE Linux Enterprise 12 SP5 Versions 19.12, 19.10 – SP1, 19.10 and 19.9
	• Dell Avamar Network Data Management Protocol (NDMP) Accelerator on SUSE Linux Enterprise 12 SP5 Versions 19.12, 19.10-SP1, 19.10, 19.9
	• Dell Avamar VMware Image Backup Proxy on SUSE Linux Enterprise 12 SP5 Versions 19.12, 19.10-SP1, 19.10, 19.9
	• Dell Networker Virtual Edition (NVE) on SUSE Linux Enterprise 12 SP5 Versions 19.9, 19.10, 19.11, 19.12
	• Dell PowerProtect DP Series Appliance (IDPA) on SUSE Linux Enterprise 12 SP5 Versions prior to 2.7.9
	• NetWorker
	  ○ Server versions 19.9 through 19.13.0.2
	  ○ Client versions 19.9 through 19.13.0.2
	  ○ Storage Node versions 19.9 through 19.13.0.2
	  ○ File-Level Recovery (FLR)
	  ○ vCenter User Interface (VCUI)

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000425769/dsa-2026-072-security-update-for-dell-avamar-dell-networker-virtual-edition-nve-and-dell-powerprotect-dp-series-appliance-dell-integrated-data-protection-appliance-idpa-multiple-third-party-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000425752/dsa-2026-048-security-update-for-dell-networker-openssl-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000425759/dsa-2026-024-security-update-for-dell-networker-multiple-third-party-component-vulnerabilities

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-48924, CVE-2025-27820, CVE-2025-8885, CVE-2025-53864, CVE-2025-8713, CVE-2025-8714, CVE-2025-8715, CVE-2025-22235, CVE-2025-22233, CVE-2025-41234, CVE-2025-41242, CVE-2025-22228)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in third party products utilized by their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NetWorker • AUTHC (Authentication Service) versions 19.9 through 19.13.0.2 • Management Console (NMC) versions 19.9 through 19.13.0.2 • Management Web UI (NWUI) versions 19.9 through 19.13.0.2 • REST APIT versions 19.9 through 19.13.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000425429/dsa-2026-023-security-update-for-dell-networker-multiple-third-party-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in the Linux Kernel utilized by their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SUSE Linux Enterprise Micro 5.3 and 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 and 5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20260411-1/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-36247, CVE-2025-14689, CVE-2025-13867, CVE-2025-36425, CVE-2025-2668, CVE-2025-33130, CVE-2025-33124, CVE-2025-13108, CVE-2025-14914)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service, Sensitive Information Disclosure and Path Traversal attacks. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Db2 version 11.5.0 to 11.5.9 and 12.1.0 to 12.1.3 DB2 Merge Backup for Linux, UNIX and Windows version 12.1.0.0 IBM WebSphere Hybrid Edition version 5.1 IBM WebSphere Application Server Liberty version 17.0.0.3 to 26.0.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7259961 https://www.ibm.com/support/pages/node/7259964 https://www.ibm.com/support/pages/node/7259963 https://www.ibm.com/support/pages/node/7259962 https://www.ibm.com/support/pages/node/7257518 https://www.ibm.com/support/pages/node/7260043 https://www.ibm.com/support/pages/node/7260100 https://www.ibm.com/support/pages/node/7258224

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21647, CVE-2024-54456, CVE-2025-21786, CVE-2025-21791, CVE-2025-38022, CVE-2025-38051, CVE-2025-38568, CVE-2025-40294, CVE-2025-40322, CVE-2025-68349, CVE-2025-38403, CVE-2025-40170, CVE-2025-40135, CVE-2025-40158, CVE-2025-40269, CVE-2022-50673, CVE-2026-22998, CVE-2025-37789, CVE-2025-37819, CVE-2025-38024, CVE-2025-38415, CVE-2025-38459, CVE-2025-38730, CVE-2025-39760, CVE-2025-40141, CVE-2025-40271, CVE-2025-40318)
Description	Red Hat 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. 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 9.6 aarch64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:2352 https://access.redhat.com/errata/RHSA-2026:2264 https://access.redhat.com/errata/RHSA-2026:2212

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Uncontrolled Resource Consumption Vulnerability (CVE-2025-8885)
Description	NetApp has released a security update addressing a resource consumption vulnerability that exists in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service (DoS) attacks. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Data Infrastructure Insights Storage Workload Security Agent (formerly Cloud Insights Storage Workload Security Agent) – Patch was issued as of 2026/02/04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250912-0012

Affected Product	**Synology**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2026-2237)
Description	Synology has released a security update addressing an information disclosure vulnerability that exists in their products. **CVE-2026-2237**: An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the APIs exposed by the documentation. Successful exploitation of this vulnerability could allow the attacker to cause damage to the targeted platform by abusing internal functionality. Synology advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Storage Manager for DSM 7.3, 7.2.2 and 7.2.1 versions prior to 1.0.1-1100
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_26_01

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.