Advisory Alert

Alert Number: AAA20260218 **Date:** February 18, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
HPE	**High**	Local Privilege Escalation Vulnerability
NetApp	**High**	Service-Side Request Forgery Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Dell	**High, Medium**	Multiple Vulnerabilities
IBM	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53677, CVE-2025-21120, CVE-2025-36598, CVE-2025-36597, CVE-2026-22769)
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 system. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Avamar Server versions 19.8 through 19.12 • Avamar Virtual Edition versions 19.8 through 19.12 • Dell PowerProtect DP Series Appliance (IDPA) versions prior to 2.7.9 • RecoverPoint for Virtual Machines versions 5.3 SP4 P1, 6.0, 6.0 SP1, 6.0 SP1 P1, 6.0 SP1 P2, 6.0 SP2, 6.0 SP2 P1, 6.0 SP3, and 6.0 SP3 P1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000347698/dsa-2025-271-security-update-for-dell-avamar-and-dell-avamar-virtual-edition-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000426773/dsa-2026-079

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Local Privilege Escalation Vulnerability (CVE-2026-23599)
Description	HPE has released a security update addressing a vulnerability that exists in HPE Aruba Networking. **CVE-2026-23599**: A local privilege-escalation vulnerability has been discovered in the HPE Aruba Networking ClearPass OnGuard Software for Linux. Successful exploitation of this vulnerability could allow a local attacker to achieve arbitrary code execution with root privileges. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE Aruba Networking ClearPass Policy Manager • 6.12.x: ClearPass 6.12.7 and below • 6.11.x: ClearPass 6.11.13 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05012en_us&docLocale=en_US

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Service-Side Request Forgery Vulnerability (CVE-2026-22048)
Description	NetApp has released a security update addressing a vulnerability that exists in StorageGRID. **CVE-2026-22048**: StorageGRID (formerly StorageGRID Webscale) versions prior to 11.9.0.12 and 12.0.0.4 with Single Sign-on enabled and configured to use Microsoft Entra ID (formerly Azure AD) as an IdP are susceptible to a Server-Side Request Forgery (SSRF) vulnerability. Successful exploit could allow an authenticated attacker with low privileges to delete configuration data or deny access to some resources. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• StorageGRID (formerly StorageGRID Webscale) versions prior to 11.9.0.12 and 12.0.0.4 (with Single Sign-On Enabled and Microsoft Entra ID in use as an IdP)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20260217-0001

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53321, CVE-2025-38111, CVE-2025-39742)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in the Linux Kernel which is utilized in their products. **CVE-2023-53321**: wifi: mac80211_hwsim: drop short frames. While technically some control frames like ACK are shorter and end after Address 1, such frames shouldn't be forwarded through wmediumd or similar userspace, so require the full 3-address header to avoid accessing invalid memory if shorter frames are passed in. **CVE-2025-38111**: net/mdiobus: Fix potential out-of-bounds read/write access .When using publicly available tools like 'mdio-tools' to read/write data from/to network interface and its PHY via mdiobus, there is no verification of parameters passed to the ioctl and it accepts any mdio address. While read/write operation should generally fail in this case, mdiobus provides stats array, where wrong address may allow out-of-bounds read/write. **CVE-2025-39742:** RDMA: hfi1: fix possible divide-by-zero in find_hw_thread_mask() The function divides number of online CPUs by num_core_siblings, and later checks the divider by zero. This implies a possibility to get and divide-by-zero runtime error. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20260566-1/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-26358, CVE-2026-26359, CVE-2026-26360, CVE-2026-26361, CVE-2026-26362, CVE-2025-46817, CVE-2025-46819, CVE-2025-49844, CVE-2025-23016, CVE-2025-61984, CVE-2025-9714, CVE-2025-7425, CVE-2024-7347, CVE-2024-33452, CVE-2025-23419, CVE-2020-16135, CVE-2023-6004, CVE-2023-6918, CVE-2025-64505, CVE-2025-64506, CVE-2025-64720, CVE-2025-65018, CVE-2025-66293, CVE-2025-4373, CVE-2025-7039, CVE-2025-13601, CVE-2025-14087, CVE-2025-14512, CVE-2026-22762)
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 system. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Unisphere for PowerMax Host Installation versions prior to 10.3.0.1 Dell PowerMax EEM Embedded Management versions prior to 10.2.0.1 Patch 10966 Dell Networking OS10 versions prior to 10.5.6.12 Avamar Server versions 19.9 through 19.10 SP1 Avamar Virtual Edition versions 19.9 through 19.10 SP1 Dell PowerProtect DP Series Appliance versions prior to 2.7.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000429268/dsa-2026-102-dell-unisphere-for-powermax-and-powermax-eem-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000429181/dsa-2026-033-security-update-for-dell-networking-os10-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000429176/dsa-2026-032-security-update-for-dell-networking-os10-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000425796/dsa-2026-053-security-update-for-dell-avamar-server-and-dell-avamar-virtual-edition-improper-limitation-of-a-pathname-to-a-restricted-directory-path-traversal-vulnerability

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2025-36009)
Description	IBM has released a security update addressing a vulnerability that exist in IBM's Db2 product. **CVE-2025-36009**: IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) could allow an unauthenticated user to cause a denial of service due to excessive use of a global variable. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Db2 Server versions 11.5.0 to 11.5.9 and 12.1.0 to 12.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7257623

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.