Advisory Alert

Alert Number: AAA20250502 **Date:** May 2, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
NetApp	**High**	Multiple Vulnerabilities
SonicWALL	**High**	Server-side request forgery Vulnerability
SUSE	**High**	Multiple Vulnerabilities
cPanel	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
HPE	**Medium**	Local Buffer Overflow Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerFlex rack RCM Versions prior to 3.6.7.1 PowerFlex Appliance IC Versions prior to IC 46.377.00 PowerFlex Appliance IC Versions prior to IC 46.382.00 Dell VxRail Appliance Versions 8.0.000 through 8.0.322
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000315723/dsa-2025-194-security-update-for-dell-powerflex-rack-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000315712/dsa-2025-193-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000314560/dsa-2025-152-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-43680, CVE-2024-28757, CVE-2024-8176, CVE-2024-45490)
Description	NetApp has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S NetApp HCI Baseboard Management Controller (BMC) - H410C NetApp HCI Baseboard Management Controller (BMC) - H610C NetApp HCI Baseboard Management Controller (BMC) - H610S NetApp HCI Baseboard Management Controller (BMC) - H615C NetApp HCI Compute Node (Bootstrap OS) NetApp SolidFire & HCI Management Node NetApp SolidFire & HCI Storage Node (Element Software) OnCommand Workflow Automation SAN Host Utilities for Windows ONTAP 9 ONTAP tools for VMware vSphere 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20241018-0004/ • https://security.netapp.com/advisory/ntap-20250328-0009/ • https://security.netapp.com/advisory/ntap-20240322-0001/ • https://security.netapp.com/advisory/ntap-20221118-0007/

Affected Product	**SonicWALL**
Severity	**High**
Affected Vulnerability	Server-side request forgery Vulnerability (CVE-2025-2170)
Description	SonicWALL has released a security update addressing an SSRF vulnerability that exists in their products. **CVE-2025-2170 -** A Server-side request forgery (SSRF) vulnerability has been identified in the SMA1000 Appliance Work Place interface, which in specific conditions could potentially enable a remote unauthenticated attacker to cause the appliance to make requests to an unintended location. SonicWALL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SMA1000 - 12.4.3-02907 (platform-hotfix) and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0008

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50205, CVE-2024-56650, CVE-2024-8805, CVE-2023-52885)
Description	SUSE has released security updates addressing multiple vulnerabilities that exists in Linux Kernel (Live Patch) System. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3 openSUSE Leap 15.4 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP3 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/2025/suse-su-20251425-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251423-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251422-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251418-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251416-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251403-1/

Affected Product	**cPanel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-32415, CVE-2025-32414, CVE-2025-216050
Description	cPanel has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of libxml2 through 2.13.7. All versions of valkey through 7.2.8.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-14-maintenance-and-security-release/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-52903, CVE-2021-29825, CVE-2023-38729, CVE-2025-27363)
Description	IBM has released a security updates addressing multiple vulnerabilities that exists in their products. **CVE-2024-52903 -** IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query. **CVE-2021-29825 -** IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. **CVE-2023-38729** – IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to sensitive information disclosure when using ADMIN_CMD with IMPORT or EXPORT. **CVE-2025-27363 -** An out of bounds write exists in FreeType versions 2.13.0 and below (newer versions of FreeType are not vulnerable) when attempting to parse font subglyph structures related to TrueType GX and variable font files. The vulnerable code assigns a signed short value to an unsigned long and then adds a static value causing it to wrap around and allocate too small of a heap buffer. The code then writes up to 6 signed long integers out of bounds relative to this buffer. This may result in arbitrary code execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 12.1.0 - 12.1.1 IBM Db2 10.5.0.x IBM Db2 11.1.4.x IBM Db2 11.5.x ServerIBM WebSphere Automation - 1.7.5, 1.8.0, 1.8.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7232336 • https://www.ibm.com/support/pages/node/6489499 • https://www.ibm.com/support/pages/node/7145721 • https://www.ibm.com/support/pages/node/7232177

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Local Buffer Overflow Vulnerability (CVE-2024-38796)
Description	HPE has released a security updates addressing a Local Buffer Overflow Vulnerability that exists in their products. **CVE-2024-38796 -** A potential security vulnerability has been identified in HPE Compute Scale-up Server 3200, Superdome Flex and Superdome Flex 280 server platform firmware. This vulnerability could be exploited to allow local buffer overflow. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Superdome Flex Server Prior to v4.5.6 HPE Superdome Flex 280 Server Prior to v2.00.12 HPE Compute Scale-up Server 3200 Prior to v1.50.120
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04856en_us&docLocale=en_US

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.