Advisory Alert

Alert Number: **AAA20250429** **Date:** **April 29, 2025**

Document Classification Level	:	Public Circulation Permitted | Public
Information Classification Level	:	TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Denial of Service (DoS) Vulnerability
Dell	**High**	Access Control Vulnerability
SUSE	**High**	Multiple Vulnerabilities
NetApp	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Denial of Service (DoS) Vulnerability (CVE-2023-25139)
Description	NetApp has released security updates addressing Denial of Service (DoS) Vulnerability that exist in products. **CVE-2023-25139 –** The NetApp products incorporate GNU C. sprintf in the GNU C Library (glibc) 2.37 is susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S • NetApp HCI Compute Node (Bootstrap OS) • NetApp SolidFire & HCI Management Node • NetApp SolidFire & HCI Storage Node (Element Software)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20230302-0010/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Access Control Vulnerability (CVE-2025-29987)
Description	Dell has released security updates addressing an Access Control Vulnerability that exists in their products. **CVE-2025-29987 –** The Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) versions prior to 8.3.0.15 contain an Insufficient Granularity of Access Control vulnerability. An authenticated user from a trusted remote client could exploit this vulnerability to execute arbitrary commands with root privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Dell DD OS 8.3 - Versions 7.7.1.0 through 8.3.0.10 • Dell DD OS 7.13.1 - Versions 7.13.1.0 through 7.13.1.20 • Dell DD OS 7.10.1 - Versions 7.10.1.0 through 7.10.1.50 • Dell PowerProtect DP Series Appliance (IDPA) - Versions 2.7.6, 2.7.7, and 2.7.8 • Dell Disk Library for mainframe DLm8500 - Version 5.4.0.0 • Dell Disk Library for mainframe DLm8700 - Version 7.0.0.0 • Dell PowerProtect DM5500 - Versions prior to 5.18.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000300899/dsa-2025-139-dell-technologies-powerprotect-data-domain-security-update-for-a-security-vulnerability

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56650, CVE-2024-53082, CVE-2024-53237, CVE-2024-56650, CVE-2024-8805, CVE-2024-53082, CVE-2024-53237, CVE-2024-56650)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in Linux Kernel RT (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	• SUSE Linux Enterprise Live Patching 15-SP6 • SUSE Linux Enterprise Real Time 15 SP6 • SUSE Linux Enterprise Server 15 SP6 • SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20251392-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251385-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251387-1/

Affected Product	**NetApp**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47554, CVE-2023-38039, CVE-2020-1749, CVE-2022-38178, CVE-2022-3996, CVE-2020-29369, CVE-2023-52340, CVE-2022-43680, CVE-2024-29131, CVE-2024-4317, CVE-2022-25147, CVE-2025-26466, CVE-2023-6237, CVE-2024-21211)
Description	NetApp 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. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250131-0010/ • https://security.netapp.com/advisory/ntap-20231013-0005/ • https://security.netapp.com/advisory/ntap-20201222-0001/ • https://security.netapp.com/advisory/ntap-20221228-0009/ • https://security.netapp.com/advisory/ntap-20230203-0003/ • https://security.netapp.com/advisory/ntap-20210115-0001/ • https://security.netapp.com/advisory/ntap-20240816-0005/ • https://security.netapp.com/advisory/ntap-20221118-0007/ • https://security.netapp.com/advisory/ntap-20241213-0001/ • https://security.netapp.com/advisory/ntap-20250328-0001/ • https://security.netapp.com/advisory/ntap-20240315-0001/ • https://security.netapp.com/advisory/ntap-20250228-0002/ • https://security.netapp.com/advisory/ntap-20240531-0007/ • https://security.netapp.com/advisory/ntap-20241018-0008/

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.