Advisory Alert

Alert Number: **AAA20250424** **Date:** **April 24, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Linux Kernel Vulnerability
NetApp	**High**	Multiple Vulnerabilities
Dell	**High**	Input Validation Vulnerability
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
Drupal	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Linux Kernel Vulnerability (CVE-2023-38429)
Description	NetApp has released security updates addressing a Linux Kernel vulnerability that exist in their products. **CVE-2023-38429 -** Multiple NetApp products incorporate Linux kernel. Linux kernel versions prior to 6.3.4 are 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	ONTAP Select Deploy administration utility ONTAP tools for VMware vSphere 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250103-0009/

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-40284, CVE-2023-40285, CVE-2023-40286, CVE-2023-40287, CVE-2023-40288, CVE-2023-40289, CVE-2023-40290, CVE-2024-0565, CVE-2023-6536, CVE-2024-12797, CVE-2025-1094, CVE-2022-1304, CVE-2023-52434, CVE-2024-10979, CVE-2024-26882, CVE-2019-17546, CVE-2024-36933, CVE-2023-52439, CVE-2024-0985, CVE-2023-6535, CVE-2023-52340, CVE-2023-6356)
Description	NetApp has released security updates addressing a Linux Kernel vulnerability 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	Active IQ Unified Manager for VMware vSphere AFF Baseboard Management Controller (BMC) - A1K/A70/A90/A700s Brocade SAN Navigator (SANnav) E-Series SANtricity OS Controller Software 11.x FAS/AFF Baseboard Management Controller (BMC) - 8300/8700/A400/C400 FAS/AFF Baseboard Management Controller (BMC) - A250/500f/C250, FAS2820 FAS/AFF Baseboard Management Controller (BMC) - A320/A800/C800/A900/9500 FAS/AFF Baseboard Management Controller (BMC) - C190/A150/A220/FAS2720/FAS2750 FAS/AFF Service Processor - A300/8200, A700/9000 NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S NetApp HCI Baseboard Management Controller (BMC) - H410C NetApp SolidFire & HCI Management Node NetApp SolidFire & HCI Storage Node (Element Software) ONTAP Select Deploy administration utility ONTAP tools for VMware vSphere 10, vSphere 9 SnapCenter Plug-in for VMware vSphere/BlueXP backup and Recovery for Virtual Machine
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20231208-0009/ • https://security.netapp.com/advisory/ntap-20240223-0002/ • https://security.netapp.com/advisory/ntap-20240415-0001/ • https://security.netapp.com/advisory/ntap-20250221-0010/ • https://security.netapp.com/advisory/ntap-20241122-0010/ • https://security.netapp.com/advisory/ntap-20250117-0009/ • https://security.netapp.com/advisory/ntap-20250110-0003/ • https://security.netapp.com/advisory/ntap-20241220-0002/ • https://security.netapp.com/advisory/ntap-20241220-0007/ • https://security.netapp.com/advisory/ntap-20240912-0006/ • https://security.netapp.com/advisory/ntap-20241227-0006/ • https://security.netapp.com/advisory/ntap-20241220-0005/ • https://security.netapp.com/advisory/ntap-20240415-0002/ • https://security.netapp.com/advisory/ntap-20240415-0003/ • https://security.netapp.com/advisory/ntap-20240816-0005/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Input Validation Vulnerability (CVE-2025-1976)
Description	Dell has released security updates addressing a Input Validation Vulnerability that exist in Dell Connectrix B-Series. This 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	Connectrix B-Series FOS - Versions 9.1.0 through 9.1.1d6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000311986/security-update-for-dell-connectrix-b-series-input-validation-vulnerability

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7449-1

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-3900, CVE-2025-3901, CVE-2025-3902, CVE-2025-3907)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Cross Site Scripting and Cross Site Request Forgery. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Prior to Drupal 10 Colorbox module 2.1.3 Bootstrap Site Alert module 8.x-1.x and 3.0.x Block Class on 4.0.x Search API Solr 4.3.10 for Drupal 8 and later
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2025-041 • https://www.drupal.org/sa-contrib-2025-042 • https://www.drupal.org/sa-contrib-2025-043 • https://www.drupal.org/sa-contrib-2025-046

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.