Advisory Alert

Alert Number: **AAA20251030** **Date:** **October 30, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
NetApp	**Critical**	Multiple Vulnerabilities
Drupal	**High**	Access Bypass Vulnerability
Dell	**High**, **Medium**	Multiple Vulnerabilities
NetApp	**High**, **Medium**, **Low**	Multiple Vulnerabilities

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 in order to compromise the affected devices. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Policy Manager for Secure Connect Gateway – Appliance Versions prior to 5.30.00.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000385220/dsa-2025-391-security-update-for-dell-secure-connect-gateway-policy-manager-for-multiple-vulnerabilities

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46604, CVE-2021-3918, CVE-2024-47685, CVE-2015-7501)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users in order to conduct Sensitive Information Disclosure, Data Modification and Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for Linux Active IQ Unified Manager for Microsoft Windows Active IQ Unified Manager for VMware vSphere E-Series SANtricity OS Controller Software 11.x E-Series SANtricity Unified Manager and Web Services Proxy NetApp HCI Baseboard Management Controller (BMC) - H410C NetApp HCI Compute Node (Bootstrap OS) ONTAP tools for VMware vSphere 10 SANtricity Storage Plugin for vCenter SnapCenter Plug-in for VMware vSphere/BlueXP Backup and Recovery for Virtual Machine StorageGRID (formerly StorageGRID Webscale)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20231110-0010 • https://security.netapp.com/advisory/ntap-20250117-0004 • https://security.netapp.com/advisory/ntap-20250613-0011 • https://security.netapp.com/advisory/ntap-20240216-0010

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Access Bypass Vulnerability (CVE-2025-12466)
Description	Drupal has released a security update addressing an Access Bypass vulnerability that exists in the Simple OAuth (OAuth2) and OpenID Connect modules. **CVE-2025-12466 -** This module introduces an OAuth 2.0 authorization server, which can be configured to protect your Drupal instance with access tokens, or allow clients to request new access tokens and refresh them. The module doesn't sufficiently respect granted scopes, it affects all access checks that are based on roles. For example: routes that have the _role requirement, can be bypassed with an access token. This vulnerability is mitigated by the fact that an attacker must have the access token in possession and the user related to the token must have the associated (role requirement) roles assigned. Drupal advises to apply this security fix at your earliest to protect systems from potential threats.
Affected Products	Simple OAuth (OAuth2) & OpenID Connect 6 Versions from 6.0.0 up to, but not including, 6.0.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2025-114

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-43939, CVE-2025-43940, CVE-2025-43941, CVE-2025-43942, CVE-2025-46422, CVE-2025-46423, CVE-2025-50059, CVE-2025-50106, CVE-2025-24855, CVE-2025-30754, CVE-2025-30749, CVE-2025-27113, CVE-2025-30761, CVE-2025-50063, CVE-2025-30752, CVE-2025-50065, CVE-2025-23166, CVE-2025-46363, CVE-2025-26465, CVE-2025-26466)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users in order to conduct OS Command Injection, Privilege Escalation, and Relative Path Traversal. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Unity Operating Environment (OE) Versions prior to 5.5.2 Dell Protection Advisor Versions 19.11 through 19.12 SP1 Secure Connect Gateway-Application Versions 5.26.00 through 5.30.00 Secure Connect Gateway-Appliance Versions 5.26.00 through 5.30.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000385307/dsa-2025-379-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000385427/dsa-2025-338-security-update-for-dell-data-protection-advisor-for-jdk-8u451-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000385239/dsa-2025-386-security-update-for-dell-secure-connect-gateway-rest-api

Affected Product	**NetApp**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users in order to compromise the affected systems. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/

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.