Advisory Alert

Alert Number: AAA20240611 **Date:** June 11, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Veeam	**Critical**	Authentication Bypass Vulnerability
Dell	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has issued security updates addressing multiple vulnerabilities that exist in Data Protection Central and PowerProtect Appliances. 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	Dell Data Protection Central Version 19.5 through 19.10.0-4 prior to DPC-OS update - 1.1.18-1 PowerProtect DP Series (IDPA) Version 2.7.6 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000225893/dsa-2024-266-security-update-for-dell-data-protection-central-for-multiple-security-vulnerabilities

Affected Product	**Veeam**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2024-29855)
Description	Veeam has issued security updates addressing an Authentication Bypass Vulnerability that exists in Veeam Recovery Orchestrator. This vulnerability allows an attacker to access the VRO web UI with administrative privileges. The attacker must know the exact username and role of an account that has an active VRO UI access token to accomplish the hijack. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Recovery Orchestrator (VRO) builds 7.0.0.337 and 7.1.0.205
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4585

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21828, CVE-2024-37130, CVE-2024-25949)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-21828** - Improper access control in some Intel(R) Ethernet Controller Administrative Tools software before version 28.3 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE-2024-37130** - Dell OpenManage Server Administrator contains a Local Privilege Escalation vulnerability via XSL Hijacking. A local low-privileged malicious user could potentially exploit this vulnerability and escalate their privilege to the admin user and gain full control of the machine. Exploitation may lead to a complete system compromise. **CVE-2024-25949** - Dell OS10 Networking Switches contain an improper authorization vulnerability. A remote authenticated attacker could potentially exploit this vulnerability leading to escalation of privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell OpenManage Server Administrator Managed Node for Windows Versions prior to 11.0.1.1 Dell Networking Switches running on Dell OS10 versions 10.5.6.x, 10.5.5.x, 10.5.4.x and 10.5.3.x Dell EMC Metro Node mn-114 and mn-215 Versions prior to 22.5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000225914/dsa-2024-264-dell-openmanage-server-administrator-omsa-security-update-for-local-privilege-escalation-via-xsl-hijacking-vulnerability • https://www.dell.com/support/kbdoc/en-us/000225922/dsa-2024-087-security-update-for-dell-networking-os10-vulnerability • https://www.dell.com/support/kbdoc/en-us/000225904/dsa-2024-265-security-update-for-dell-emc-metro-node-for-intel-ethernet-controllers-adapters-vulnerability

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.