Advisory Alert

Alert Number: AAA20240708 **Date:** July 8, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
NetApp	**Medium**	Information Disclosure Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-35235,CVE-2024-33602,CVE-2024-33601,CVE-2024-33600,CVE-2024-33599,CVE-2024-32487,CVE-2024-28835,CVE-2024-28834,CVE-2024-27389,CVE-2024-27043,CVE-2024-26903,CVE-2024-26898,CVE-2024-26816,CVE-2024-26792,CVE-2024-26773,CVE-2024-26766,CVE-2024-26764,CVE-2024-26739,CVE-2024-26733,CVE-2024-26727,CVE-2024-26704,CVE-2024-26689,CVE-2024-26688,CVE-2024-26687,CVE-2024-26642,CVE-2024-26614,CVE-2024-26610,CVE-2024-26601,CVE-2024-25742,CVE-2024-2511,CVE-2024-25062,CVE-2024-2398,CVE-2024-23850,CVE-2024-23848,CVE-2024-23307,CVE-2024-22099,CVE-2024-21094,CVE-2024-21085,CVE-2024-21068,CVE-2024-21012,CVE-2024-21011,CVE-2024-2004,CVE-2024-0841,CVE-2024-0567,CVE-2024-0553,CVE-2024-0450,CVE-2023-7207,CVE-2023-7192,CVE-2023-7042,CVE-2023-6597,CVE-2023-6270,CVE-2023-5981,CVE-2023-5388,CVE-2023-52628,CVE-2023-52616,CVE-2023-52607,CVE-2023-52591,CVE-2023-52590,CVE-2023-52500,CVE-2023-52476,CVE-2023-52425,CVE-2023-4881,CVE-2023-28859,CVE-2023-28858,CVE-2023-0160,CVE-2022-48668,CVE-2022-48667,CVE-2022-48663,CVE-2022-48662,CVE-2022-48660,CVE-2022-48657,CVE-2022-48656,CVE-2022-48655,CVE-2022-48654,CVE-2022-48653,CVE-2022-48651,CVE-2022-48650,CVE-2022-48648,CVE-2022-48647,CVE-2022-48638,CVE-2022-48637,CVE-2022-48631,CVE-2021-47219,CVE-2021-47218,CVE-2021-47217,CVE-2021-47216,CVE-2021-47215,CVE-2021-47212,CVE-2021-47211,CVE-2021-47210,CVE-2021-47209,CVE-2021-47207,CVE-2021-47206,CVE-2021-47205,CVE-2021-47204,CVE-2021-47203,CVE-2021-47202,CVE-2021-47201,CVE-2021-47200,CVE-2021-47199,CVE-2021-47198,CVE-2021-47197,CVE-2021-47196,CVE-2021-47195,CVE-2021-47194,CVE-2021-47193,CVE-2021-47192,CVE-2021-47191,CVE-2021-47189,CVE-2021-47188,CVE-2021-47187,CVE-2021-47185,CVE-2021-47184,CVE-2021-47183,CVE-2021-47182,CVE-2021-47181,CVE-2021-47047,CVE-2021-3521,CVE-2021-33813,CVE-2018-6913,CVE-2018-6798, CVE-2024-37081, CVE-2024-37080, CVE-2024-37079)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products that in turn affect Dell products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell EMC VxRail Appliance - 7.0.x versions prior to 7.0.521
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226716/dsa-2024-288-security-update-for-dell-vxrail-7-0-521-multiple-third-party-component-vulnerabilities

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2024-21993)
Description	NetApp has released security updates addressing an Information Disclosure Vulnerability that exist in their products. Exploitation of this vulnerability could allow an authenticated attacker to discover plaintext credentials. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SnapCenter versions prior to 5.0p1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240705-0007/

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.