Advisory Alert

Alert Number: AAA20240703 **Date:** July 3, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Juniper	**High**	Denial-of-Service vulnerability
Dell	**High**	Multiple Vulnerabilities
Apache HTTP Server	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38545, CVE-2023-38546, CVE-2024-37079, CVE-2024-37080, CVE-2024-37081)
Description	Dell has released security updates addressing multiple vulnerabilities in third-party components running on their 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 NetWorker Version 19.10 Dell NetWorker Versions 19.9 through 19.9.0.6 Dell NetWorker Versions 19.8 through 19.8.0. 4 Dell NetWorker Versions prior to 19.8 PowerStore 1000X, running on vCenter Versions prior to 7.0U3r PowerStore 3000X, running on vCenter Versions prior to 3.6.0.0-2145637 PowerStore 5000X, running on vCenter Versions prior to 7.0U3r PowerStore 7000X, running on vCenter Versions prior to 7.0U3r PowerStore 9000X, running on vCenter Versions prior to 7.0U3r PowerStore 500T, running on vCenter Versions prior to 8.0U2d PowerStore 1000T, running on vCenter Versions prior to 8.0U2d PowerStore 1200T, running on vCenter Versions prior to 8.0U2d PowerStore 3000T, running on vCenter Versions prior to 8.0U2d PowerStore 3200Q, running on vCenter Versions prior to 8.0U2d PowerStore 3200T, running on vCenter Versions prior to 8.0U2d PowerStore 5000T, running on vCenter Versions prior to 8.0U2d PowerStore 5200T, running on vCenter Versions prior to 8.0U2d PowerStore 7000T, running on vCenter Versions prior to 8.0U2d PowerStore 9000T, running on vCenter Versions prior to 8.0U2d PowerStore 9200T, running on vCenter Versions prior to 8.0U2d
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000223914/dsa-2024-166-security-update-for-dell-networker-curl-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000226626/dsa-2024-283-dell-powerstore-family-security-update-for-vmware-vulnerabilities

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Denial-of-Service vulnerability (CVE-2024-21586)
Description	Juniper has released security updates addressing an Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series. If exploited, an unauthenticated, network-based attacker could cause a Denial-of-Service (DoS) by continuously sending specific valid traffic destined for the device. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS on SRX Series: 21.4 versions before 21.4R3-S7.9 22.1 versions before 22.1R3-S5.3 22.2 versions before 22.2R3-S4.11 22.3 versions before 22.3R3 22.4 versions before 22.4R3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-07-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-Specific-valid-traffic-leads-to-a-PFE-crash-CVE-2024-21586?language=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5868, CVE-2023-5869, CVE-2023-5870, CVE-2024-0985, CVE-2023-43804, CVE-2020-26137, CVE-2023-45803, CVE-2024-2658, CVE-2023-50782, CVE-2023-52425, CVE-2023-0215, CVE-2023-48795)
Description	Dell 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. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerVault ME50xx Storage Versions prior to ME5.1.2.1.0 Dell NetWorker, Versions 19.10 through 19.10.0.3 Dell NetWorker, Versions 19.9 through 19.9.0.6 Dell NetWorker, Versions 19.8 through 19.8.0.4 Dell NetWorker, Versions prior to 19.8 Dell NetWorker Virtual Edition Versions 19.10 through 19.10.0.3 Dell NetWorker Virtual Edition Versions 19.9 through 19.9.0.6 Dell NetWorker Virtual Edition Versions 19.8 through 19.8.0.4 Dell NetWorker Virtual Edition Versions prior to 19.8 Dell EMC License Server Version 3.6.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000226627/dsa-2024-302-dell-powervault-security-update-for-me5-storage • https://www.dell.com/support/kbdoc/en-us/000226582/dsa-2024-012-security-update-for-dell-networker-virtual-edition-networker-management-console-multiple-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000226576/dsa-2024-007-security-update-for-dell-networker-license-server-vulnerabilities

Affected Product	**Apache HTTP Server**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36387, CVE-2024-38472, CVE-2024-38473, CVE-2024-38474, CVE-2024-38475, CVE-2024-38476, CVE-2024-38477, CVE-2024-39573)
Description	Apache has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Null Pointer dereference, Authentication bypass, Information disclosure, Denial of Service, Local script execution Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache HTTP Server versions below 2.4.60
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

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.