Advisory Alert

Alert Number: AAA20250307 **Date:** March 7, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45142, CVE-2023-7108, CVE-2022-1996, CVE-2022-48911, CVE-2022-48945, CVE-2024-36971, CVE-2024-41087, CVE-2024-44946, CVE-2024-45003, CVE-2024-45021, CVE-2024-46695, CVE-2023-50782, CVE-2024-7348, CVE-2024-6232, CVE-2024-45310)
Description	Dell has released security updates addressing multiple Vulnerabilities that exist in third party products which affect Dell PowerStore servers. 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	PowerStore 500T PowerStoreT OS Versions prior to 4.0.1.2-2445526 PowerStore 1000T PowerStoreT OS Versions prior to 4.0.1.2-2445526 PowerStore 1200T PowerStoreT OS Versions prior to 4.0.1.2-2445526 PowerStore 3000T PowerStoreT OS Versions prior to 4.0.1.2-2445526 PowerStore 3200Q PowerStoreT OS Versions prior to 4.0.1.2-2445526 PowerStore 3200T PowerStoreT OS Versions prior to 4.0.1.2-2445526 PowerStore 5000T PowerStoreT OS Versions prior to 4.0.1.2-2445526 PowerStore 5200T PowerStoreT OS Versions prior to 4.0.1.2-2445526 PowerStore 7000T PowerStoreT OS Versions prior to 4.0.1.2-2445526 PowerStore 9000T PowerStoreT OS Versions prior to 4.0.1.2-2445526 PowerStore 9200T PowerStoreT OS Versions prior to 4.0.1.2-2445526
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000291612/dsa-2025-117-dell-powerstore-t-security-update-for-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-52798, CVE-2024-47764)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-52798 -** path-to-regexp turns path strings into a regular expressions. In certain cases, path-to-regexp will output a regular expression that can be exploited to cause poor performance. The regular expression that is vulnerable to backtracking can be generated in the 0.1.x release of path-to-regexp. Upgrade to 0.1.12. This vulnerability exists because of an incomplete fix for CVE-2024-45296. **CVE-2024-47764 -** jshttp cookie could allow a remote attacker to bypass security restrictions, caused by improper input validation by the cookie name, path, and domain. By sending a specially crafted request, an attacker could exploit this vulnerability to alter other fields of the cookie. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Pulse App Version(s) - 1.0.0 - 2.2.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7184955

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.