# Advisory Alert

**Alert Number:** **AAA20241213** **Date:** **December 13, 2024**

**Document Classification Level** : Public Circulation Permitted | Public

**Information Classification Level** : TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Dell** | **Critical** | Multiple Vulnerabilities |
| **Dell** | **High** | Multiple Vulnerabilities |
| **Ubuntu** | **High, Medium, Low** | Multiple Vulnerabilities |
| **Cisco** | **Medium** | Uncontrolled Resource Consumption Vulnerability |
| **IBM** | **Medium, Low** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell products. These vulnerabilities could be exploited by malicious users to compromise the affected system.<br>Dell advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | PowerFlex rack RCM Versions prior to 3.8.1.0<br>PowerFlex appliance IC Versions prior to 46.381.00<br>Dell Data Lakehouse System Software Versions 1.0.0.0 and 1.1.0.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.dell.com/support/kbdoc/en-us/000259564/dsa-2024-474-security-update-for-dell-powerflex-rack-multiple-third-party-component-vulnerabilities<br>• https://www.dell.com/support/kbdoc/en-us/000259574/dsa-2024-484-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities<br>• https://www.dell.com/support/kbdoc/en-us/000240535/dsa-2024-419-security-update-for-dell-data-lakehouse-system-software-for-multiple-third-party-component-vulnerabilities |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell products. These vulnerabilities could be exploited by malicious users to compromise the affected system.<br>Dell advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Dell Edge Gateway 5000 BIOS Versions prior to 1.29.0<br>Edge Gateway 3000 series BIOS Versions prior to 1.19.0<br>Embedded Box PC 3000 BIOS Versions prior to 1.25.0<br>PowerStoreT OS Versions prior to 4.0.1.0-2408234 running on:<br>• PowerStore 500T<br>• PowerStore 1000T<br>• PowerStore 1200T<br>• PowerStore 3000T<br>• PowerStore 3200Q<br>• PowerStore 3200T<br>• PowerStore 5000T<br>• PowerStore 5200T<br>• PowerStore 7000T<br>• PowerStore 9000T<br>• PowerStore 9200T |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.dell.com/support/kbdoc/en-us/000227595/dsa-2024-355<br>• https://www.dell.com/support/kbdoc/en-us/000250483/dsa-2024-462-dell-powerstore-t-security-update-for-multiple-vulnerabilities |

| Affected Product | **Ubuntu** |
|---|---|
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux Kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system.<br>Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Ubuntu 18.04<br>Ubuntu 20.04<br>Ubuntu 22.04<br>Ubuntu 24.04 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://ubuntu.com/security/notices/USN-7159-1<br>• https://ubuntu.com/security/notices/USN-7154-1 |

| Affected Product | **Cisco** |
|---|---|
| Severity | **Medium** |
| Affected Vulnerability | Uncontrolled Resource Consumption Vulnerability (CVE-2023-20268) |
| Description | Cisco has released security updates addressing an Uncontrolled Resource Consumption Vulnerability that exists in Cisco Access Point Software.<br>**CVE-2023-20268** - This vulnerability is due to insufficient management of resources when handling certain types of traffic. An attacker could exploit this vulnerability by sending a series of specific wireless packets to an affected device. A successful exploit could allow the attacker to consume resources on an affected device. A sustained attack could lead to the disruption of the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel and intermittent loss of wireless client traffic.<br>Cisco advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | • Cisco Wireless LAN Controller Software Releases 8.10, 8.9 and earlier<br>• Cisco Catalyst 9800 Wireless Controller Software Releases 17.11, 17.10, 17.9, 17.8, 17.6, 17.5, 17.4, 17.3, 17.2 and earlier<br>• Cisco Business 100 and 200 Series AP Software Releases 10.10.1, 10.9.1 and earlier<br>• Cisco Business 150 Series AP Software Releases 10.6.2, 10.5.2 and earlier |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-dos-capwap-DDMCZS4m |

| Affected Product | **IBM** |
|---|---|
| Severity | **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-21217, CVE-2024-21208, CVE-2024-10917, CVE-2024-9143, CVE-2024-21085, CVE-2024-21012, CVE-2024-3933) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, bypass security restrictions, Arbitrary Code Execution.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Db2 Query Management Facility versions 13.1.2 and 13.1.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7178758<br>• https://www.ibm.com/support/pages/node/7178756 |

**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.**