Advisory Alert

Alert Number: **AAA20241217** **Date:** **December 17, 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
IBM	**High,** **Medium,** **Low**	Multiple Vulnerabilities
Ubuntu	**Medium**	Linux kernel vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update 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 Storage Resource Manager- Vapp Versions prior to 5.0.2.1 Dell Storage Monitoring and Reporting –Vapp Versions prior to 5.0.2.1 Dell Storage Resource Manager Windows/Linux update Versions prior to 5.0.2.1 Dell Storage Monitoring and Reporting Windows/Linux update Versions prior to 5.0.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000260781/dsa-2024-479-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2021-33164, CVE-2024-24853, CVE-2023-39538, CVE-2023-39539, CVE-2024-21781)
Description	Dell has released a security update 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	PowerScale Archive A300 -PowerScale Node Firmware Package Versions prior to 12.4.1 PowerScale Archive A3000- PowerScale Node Firmware Package Versions prior to 12.4.1 PowerScale Hybrid H700 -PowerScale Node Firmware Package Versions prior to 12.4.1 PowerScale Hybrid H7000 -PowerScale Node Firmware Package Versions prior to 12.4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000260794/dsa-2024-455-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2024-36889, CVE-2024-26629, CVE-2024-0841, CVE-2023-52455, CVE-2021-47289, CVE-2023-52489, CVE-2024-41064, CVE-2023-0597, CVE-2024-40972, CVE-2023-2269, CVE-2023-42754, CVE-2023-3161, CVE-2024-26633, CVE-2024-26671, CVE-2023-1077, CVE-2024-42152, CVE-2024-41055, CVE-2024-6119, CVE-2023-52581, CVE-2023-3640, CVE-2024-38601, CVE-2024-10979, CVE-2024-21147, CVE-2024-21145, CVE-2024-21140, CVE-2024-21138, CVE-2024-21131, CVE-2024-26640, CVE-2023-52474, CVE-2023-52610, CVE-2023-52472, CVE-2023-6915, CVE-2023-52476, CVE-2024-24855, CVE-2024-26826, CVE-2023-1206, CVE-2023-52580, CVE-2024-40978, CVE-2024-40954, CVE-2023-52620, CVE-2024-40959, CVE-2023-3268, CVE-2023-39194, CVE-2023-45863, CVE-2024-40960, CVE-2023-6622)
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, sensitive information disclosure, arbitrary code execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale System Versions 6.1.0.0 - 6.1.9.4 IBM Storage Scale System Versions 6.2.0.0 - 6.2.1.1 IBM WebSphere Application Server version 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7173128 • https://www.ibm.com/support/pages/node/7179055 • https://www.ibm.com/support/pages/node/7179045

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Linux kernel vulnerability (CVE-2024-53057)
Description	Ubuntu has released a security update addressing a Linux kernel vulnerability that exists in the network traffic control subsystem of Ubuntu 14.04. If exploited, malicious users can cause the system to crash by sending specially crafted network traffic. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7163-1

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.