Advisory Alert

Alert Number: **AAA20250421** **Date:** **April 21, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Lenovo	**High**	Code Injection Vulnerability
Dell	**High**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
Commvault	**Medium**	SQL Injection Vulnerability
FortiGuard	**Low**	Information Disclosure Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell Storage Resource Manager and Dell Storage Monitoring and Reporting firmware. 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 5.1.0.0 Dell Storage Resource Manager Windows/Linux Versions prior to 5.1.0.0 Dell Storage Monitoring and Reporting Vapp Versions prior to 5.1.0.0 Dell Storage Monitoring and Reporting Windows/Linux Versions prior to 5.1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000309323/dsa-2025-165-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Code Injection Vulnerability (CVE-2025-1976)
Description	Lenovo has released security updates addressing a Code Injection Vulnerability that exists in their products which uses Update Brocade Fabric OS. These vulnerabilities could be exploited by malicious users to compromise the affected system. Lenovo advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following products if they are running on Brocade Fabric OS versions 9.1.0 through 9.1.1d6 • Brocade - 300 FC SAN Switch • Brocade - 6505 FC SAN Switch • Brocade - 6510 FC SAN Switch • Brocade X7-4 64G FC Director • Brocade X7-8 64G FC Director • Lenovo - B300 FC SAN Switch • Lenovo - B6505 FC SAN Switch • Lenovo - B6510 FC SAN Switch • Lenovo ThinkSystem DB400D FC Switch • Lenovo ThinkSystem DB610S FC Switch • Lenovo ThinkSystem DB620S FC Switch • Lenovo ThinkSystem DB630S FC Switch • Lenovo ThinkSystem DB720S FC Switch • Lenovo ThinkSystem DB730S FC Switch • Lenovo ThinkSystem DB800D FC Switch
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-194716

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-8805, CVE-2023-5678, CVE-2023-6129, CVE-2024-0727, CVE-2023-46218, CVE-2023-46219, CVE-2024-9681, CVE-2023-52425, CVE-2023-52426)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell NetWorker vProxy. 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	NetWorker vProxy OVA Version 19.12 and prior to 19.11.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000309762/dsa-2025-187-security-update-for-dell-networker-vproxy-multiple-third-party-component-vulnerabilities

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-12369, CVE-2025-23367, CVE-2024-3884)
Description	Red Hat 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. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:3989 • https://access.redhat.com/errata/RHSA-2025:3990 • https://access.redhat.com/errata/RHSA-2025:3992

Affected Product	**Commvault**
Severity	**Medium**
Affected Vulnerability	SQL Injection Vulnerability
Description	Commvault has released security updates addressing an SQL Injection Vulnerability that exists in CommServe and Web Server installation. These vulnerabilities could be exploited by malicious users to compromise the affected system. Commvault advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Commvault Linux and Windows versions: • 11.32.0 - 11.32.93 • 11.36.0 - 11.36.51 • 11.38.0 - 11.38.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2025_04_2.html

Affected Product	**FortiGuard**
Severity	**Low**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2024-50564)
Description	FortiGuard has released security updates addressing a use of hard-coded cryptographic key vulnerability in FortiClient Windows. This vulnerability may allow a low-privileged user to decrypt interprocess communication via monitoring named pipe. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiClientWindows version 7.4.0 FortiClientWindows versions 7.2.0 through 7.2.8 FortiClientWindows 7.0 all versions FortiClientWindows 6.4 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-216

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.