Advisory Alert

Alert Number: AAA20250701 **Date:** July 1, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Latitude 3420 – ThinOS 2411 Latitude 3440 – ThinOS 2411 Latitude 5440 – ThinOS 2411 Latitude 5450 – ThinOS 2411 NetWorker Server, NetWorker Client, NetWorker Storage Node, NetWorker Web UI, File Level Recovery (FLR), NetWorker Authentication Server, NetWorker vCenter User Interface (VCUI), NetWorker RESTAPI - Versions 19.12 through 19.12.0.1, Versions prior to 19.11.0.5 ObjectScale - Versions prior to 4.0.0.1 OptiPlex 3000 Thin Client – ThinOS 2411 OptiPlex 5400 All-In-One – ThinOS 2411 OptiPlex AIO 7410 – ThinOS 2411 OptiPlex AIO 7420 – ThinOS 2411 PowerScale OneFS - Versions 9.5.0.0 through 9.10.0.1, Versions 9.7.0.0 through 9.7.1.7, Versions 9.5.0.0 through 9.5.1.2, Versions 9.5.0.0 through 9.5.1.3 Wyse 5070 Thin Client – ThinOS 2411 Wyse 5470 All-In-One Thin Client – ThinOS 2411 Wyse 5470 Mobile Thin Client – ThinOS 241
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000289886/dsa-2025-107 • https://www.dell.com/support/kbdoc/en-us/000337969/dsa-2025-234-security-update-for-dell-networker-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000338043/dsa-2025-258-security-update-for-dell-networker-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000339112/dsa-2025-243-security-update-for-dell-objectscale-4-0-0-1-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000326339/dsa-2025-208-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5, 15 SP5 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502173-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502171-1/

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27113, CVE-2024-0161, CVE-2011-1473, CVE-2011-5094, CVE-2024-0154, CVE-2024-0173)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000338768/dsa-2025-266-security-update-for-dell-networker-libxml2-component-vulnerability • https://www.dell.com/support/kbdoc/en-us/000222979/dsa-2024-006-security-update-for-dell-poweredge-server-bios-for-an-improper-smm-communication-buffer-verification-vulnerability • https://www.dell.com/support/kbdoc/en-us/000337983/dsa-2025-222-security-update-for-dell-networker-management-console-openssl-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000222898/dsa-2024-034-security-update-for-dell-poweredge-server-bios-for-an-improper-parameter-initialization-vulnerability

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52933, CVE-2025-21883, CVE-2025-21961, CVE-2025-22104, CVE-2022-49111, CVE-2022-49114, CVE-2022-49122)
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 affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:9880 • https://access.redhat.com/errata/RHSA-2025:9896 • https://access.redhat.com/errata/RHSA-2025:10005

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.