Advisory Alert

Alert Number: **AAA20250506** **Date:** **May 6, 2025**

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

Information Classification Level **:** TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Memory Corruption Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Memory Corruption Vulnerability (CVE-2025-21927)
Description	Red Hat has released Memory Corruption Vulnerability that exists in kernel-rt packages. **CVE-2025-21927 -** In the Linux kernel, the following vulnerability has been resolved: nvme-tcp: fix potential memory corruption in nvme_tcp_recv_pdu() nvme_tcp_recv_pdu() doesn't check the validity of the header length. When header digests are enabled, a target might send a packet with an invalid header length (e.g. 255), causing nvme_tcp_verify_hdgst() to access memory outside the allocated area and cause memory corruptions by overwriting it with the calculated digest. Fix this by rejecting packets with an unexpected header length. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le • Red Hat Enterprise Linux for Power, little endian 9 ppc64le • Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 • Red Hat Enterprise Linux for x86_64 9 x86_64 • Red Hat Enterprise Linux Server - AUS 9.2 x86_64 • Red Hat Enterprise Linux Server - AUS 9.4 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:4471 • https://access.redhat.com/errata/RHSA-2025:4469 • https://access.redhat.com/errata/RHSA-2025:4496 • https://access.redhat.com/errata/RHSA-2025:4497 • https://access.redhat.com/errata/RHSA-2025:4498 • https://access.redhat.com/errata/RHSA-2025:4499

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50205, CVE-2024-56650, CVE-2024-8805, CVE-2023-52885)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in Linux Kernel (Live Patch) System. 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 15.3 • openSUSE Leap 15.4 • SUSE Linux Enterprise High Performance Computing 15 SP3 • SUSE Linux Enterprise High Performance Computing 15 SP4 • SUSE Linux Enterprise Live Patching 15-SP3 • SUSE Linux Enterprise Live Patching 15-SP4 • SUSE Linux Enterprise Micro 5.1 • SUSE Linux Enterprise Micro 5.2 • SUSE Linux Enterprise Server 15 SP3 • SUSE Linux Enterprise Server for SAP Applications 15 SP3 • SUSE Linux Enterprise Micro 5.3 • SUSE Linux Enterprise Micro 5.4 • SUSE Linux Enterprise Real Time 15 SP4 • SUSE Linux Enterprise Server 15 SP4 • SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20251445-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251444-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251449-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251448-1/

Affected Product	**Dell**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-48795, CVE-2022-48285, CVE-2021-23413, CVE-2020-11022, CVE-2020-11023, CVE-2015-9251, CVE-2020-7676, CVE-2025-22479, CVE-2025-22477, CVE-2025-22478, CVE-2025-22476, CVE-2025-23379)
Description	Dell has released security updates addressing multiple vulnerabilities in the Dell Storage Manager product. If exploited, these vulnerabilities could lead to script injection, privilege escalation, information disclosure, and information tampering. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Storage Manager Versions prior to 2020 R1.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000317318/dsa-2025-191-security-update-for-storage-center-dell-storage-manager-vulnerabilities

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.