TLP: WHITE

Advisory Alert

Alert Number: AAA20260304 **Date:** March 4, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-43265, CVE-2025-43240, CVE-2025-43228, CVE-2025-43227, CVE-2025-43216, CVE-2025-43212, CVE-2025-43211, CVE-2025-31278, CVE-2025-31273, CVE-2025-58364, CVE-2025-58060, CVE-2025-47808, CVE-2025-47807, CVE-2025-47806, CVE-2025-48060, CVE-2024-53427, CVE-2024-23337, CVE-2025-4969, CVE-2025-4948, CVE-2025-4945, CVE-2025-32914, CVE-2025-32907, CVE-2024-45615, CVE-2024-45617, CVE-2024-45620, CVE-2024-45619, CVE-2024-45618, CVE-2024-8443, CVE-2024-45616, CVE-2025-57812, CVE-2025-64503, CVE-2025-7462, CVE-2025-59800, CVE-2025-59799, CVE-2025-59798, CVE-2025-52885, CVE-2025-7709, CVE-2025-26403, CVE-2025-20109, CVE-2025-20053, CVE-2025-22840, CVE-2025-22889, CVE-2025-32086, CVE-2025-24305, CVE-2025-21090, CVE-2025-22839, CVE-2025-62230, CVE-2025-62231, CVE-2025-62229, CVE-2025-11083, CVE-2025-1147, CVE-2025-5245, CVE-2025-11082, CVE-2025-5244, CVE-2025-1182, CVE-2025-7545, CVE-2025-7546, CVE-2025-1148, CVE-2025-8225, CVE-2025-3198, CVE-2024-10963, CVE-2026-0899, CVE-2026-0900, CVE-2026-0901, CVE-2026-0902, CVE-2026-0903, CVE-2026-0904, CVE-2026-0905, CVE-2026-0906, CVE-2026-0907, CVE-2026-0908, CVE-2025-43342, CVE-2025-43343, CVE-2016-5180, CVE-2017-1000381, CVE-2020-8277, CVE-2021-3672, CVE-2022-4904, CVE-2023-31124, CVE-2023-31130, CVE-2023-31147, CVE-2023-32067, CVE-2024-25629, CVE-2022-25255, CVE-2022-25634, CVE-2023-32763)
Description	Dell has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products that utilize the ThinOS 10 Firmware.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000430056/dsa-2026-110

Affected Product	**Red Hat**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37861, CVE-2025-38415, CVE-2025-38459, CVE-2025-39760, CVE-2025-39817, CVE-2025-39993, CVE-2025-40271, CVE-2022-50673, CVE-2025-68349, CVE-2026-23074)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the Linux Kernel utilized by their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le 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 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64 Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power little endian 7 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-2026:3692 • https://access.redhat.com/errata/RHSA-2026:3685

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22285, CVE-2026-22760, CVE-2026-26949, CVE-2024-4603, CVE-2023-2975, CVE-2026-25906, CVE-2025-12418, CVE-2025-11731)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Unauthorized Access, Denial of Service and Privilege Escalation attacks. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Device Management Agent (DDMA) versions prior to 26.02 Dell Pro Micro / QCM1255 versions prior to 1.10.2 Dell Pro Slim / QCS1255 versions prior to 1.10.2 Dell Pro Tower / QCT1255 versions prior to 1.10.2 Dell Pro 13 Plus PB13255 versions prior to 1.10.2 Dell Pro 14 Plus PB14255 versions prior to 1.10.2 Dell Pro 16 Plus PB16255 versions prior to 1.10.2 Dell Pro Max 14 MC14255 versions prior to 1.8.0 Dell Pro Max 16 MC16255 versions prior to 1.8.0 Dell Pro 14 PC14255 versions prior to 1.11.1 Dell Pro 16 PC16255 versions prior to 1.11.1 Dell Optimizer versions 6.0.0.0 to 6.3.0.0 Dell Connected Service Delivery SubAgent versions prior to 1.1.0.0 Dell Command Monitor versions prior to 10.13.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000429177/dsa-2026-105 • https://www.dell.com/support/kbdoc/en-us/000404482/dsa-2026-021-security-update-for-dell-client-platform-bios-for-multiple-openssl-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000427608/dsa-2026-094 • https://www.dell.com/support/kbdoc/en-us/000428756/dsa-2026-098 • https://www.dell.com/support/kbdoc/en-us/000429172/dsa-2026-104

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.