Advisory Alert

Alert Number: AAA20260626 **Date:** June 26, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Check Point	**High**	Multiple Vulnerabilities

Description

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-47912, CVE-2025-61723, CVE-2025-61725, CVE-2025-61726, CVE-2025-61727, CVE-2025-61729, CVE-2025-61730, CVE-2025-58185, CVE-2025-58187, CVE-2025-58188, CVE-2025-58189, CVE-2025-47907, CVE-2025-4674, CVE-2023-45288, CVE-2024-27304, CVE-2025-66168, CVE-2021-28041, CVE-2023-51767)
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 systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell OpenManage Enterprise Modular Versions prior to 2.20.20
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000481724/dsa-2026-298-security-update-for-dell-openmanage-enterprise-modular-vulnerabilities

Vendor	**Dell**
Severity	**High**
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 the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	iDRAC10 Versions prior to 1.3.0.10.51 PowerSwitch Z9864F-ON Firmware Versions prior to 3.5.0 Below Products Versions prior to 2606: • AX-770 • AX-670 • AX-760 • AX-660 • AX-4510C • AX-4520C • AX-6515 • AX-7525 • AX-650 • AX-750 • AX-640 • AX-740xd
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000481646/dsa-2026-270-security-update-for-dell-idrac10-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000481561/dsa-2026-264-security-update-for-dell-ax-system-for-azure-local-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000481535/dsa-2026-296-security-update-for-dell-networking-products-for-multiple-vulnerabilities

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-9256, CVE-2026-31636, CVE-2026-43038, CVE-2026-43198, CVE-2026-43414, CVE-2026-45898, CVE-2026-46117, CVE-2026-46145, CVE-2026-46135)
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 systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Red Hat Enterprise Linux for x86_64 10 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 • Red Hat Enterprise Linux for IBM z Systems 10 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.2 s390x • Red Hat Enterprise Linux for Power, little endian 10 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le • Red Hat Enterprise Linux for ARM 64 10 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.2 aarch64 • Red Hat CodeReady Linux Builder for x86_64 10 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le • Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 • Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.2 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.2 ppc64le • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.2 s390x • Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.2 aarch64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.2 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.2 s390x • Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le • Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 • Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 10.2 aarch64 • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le • Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 10.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:29874 https://access.redhat.com/errata/RHSA-2026:30129

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-10263, CVE-2025-68324, CVE-2026-23392, CVE-2026-31500, CVE-2026-31697, CVE-2026-31698, CVE-2026-31699, CVE-2026-31759, CVE-2026-31771, CVE-2026-43023, CVE-2026-43074, CVE-2026-43077, CVE-2026-43198, CVE-2026-45878, CVE-2026-45886, CVE-2026-45932, CVE-2026-45984, CVE-2026-46037, CVE-2026-46090, CVE-2026-46120, CVE-2026-46123, CVE-2026-46150, CVE-2026-46159, CVE-2026-46197, CVE-2026-46209, CVE-2026-46227, CVE-2026-46273, CVE-2026-31473, CVE-2026-31613, CVE-2026-46116, CVE-2026-31405, CVE-2026-31758, CVE-2026-43366, CVE-2026-43503, CVE-2026-45970, CVE-2026-46021, CVE-2026-46113)
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 systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 and LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Micro 5.3, 5.4 and 5.5 SUSE Linux Enterprise Micro for Rancher 5.3 and 5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262632-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262631-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262630-1/

Vendor	**Check Point**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-48133, CVE-2026-50752)
Description	Check Point has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-48133:** When the Identity Awareness blade is enabled with Browser-Based Authentication, an unauthenticated user may be able to read certain internal files on the Security Gateway. **CVE-2026-50752:** A vulnerability in the certificate validation logic of the deprecated IKEv1 key exchange method may lead to a man-in-the-middle attack on the VPN site-to-site configuration. Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All releases from R81.10 and below R82.10 Jumbo Hotfix Take 19 or below R82 Jumbo Hotfix Take 103 or below R81.20 Jumbo Hotfix Take 141 or below R81.10 (EOS) R81 (EOS) R80.40 (EOS) Spark Firewalls: R80.20.X (EOS), R81.10.X, R82.00.X
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk184993 https://support.checkpoint.com/results/sk/sk185035

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.