Advisory Alert

Alert Number: AAA20260506 **Date:** May 6, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Palo Alto Networks	**Critical**	Buffer Overflow Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Juniper Networks	**High**	Multiple Vulnerabilities
cPanel	**High, Medium, Low**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities
Dell	**Low**	Insufficient Logging Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42444, CVE-2024-7344, CVE-2024-45332, CVE-2024-28047, CVE-2024-28956, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-0464, CVE-2023-0465, CVE-2023-6237, CVE-2024-5535, CVE-2024-6119, CVE-2024-13176, CVE-2024-38796)
Description	Dell has released a security update addressing multiple vulnerabilities that exists in the third party components of their product. 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	PowerScale A300 – Versions prior to 13.2.3 PowerScale A3000 – Versions prior to 13.2.3 PowerScale H700 – Versions prior to 13.2.3 PowerScale H7000 – Versions prior to 13.2.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000461405/dsa-2026-127-security-update-for-dell-powerscale-onefs-multiple-third-party-component-vulnerabilities

Affected Product	**Palo Alto Networks**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-0300)
Description	Palo Alto Networks has released a security updates addressing a vulnerability that exists in their product. **CVE-2026-0300:** A buffer overflow vulnerability in the User-ID™ Authentication Portal (aka Captive Portal) service of Palo Alto Networks PAN-OS software allows an unauthenticated attacker to execute arbitrary code with root privileges on the PA-Series and VM-Series firewalls by sending specially crafted packets. Palo Alto Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 12.1 Versions prior to 12.1.4-h5 & 12.1.7 PAN-OS 11.2 Versions prior to 11.2.4-h17, 11.2.7-h13, 11.2.10-h6, 11.2.12 PAN-OS 11.1 Versions prior to 11.1.4-h33, 11.1.6-h32, 11.1.7-h6, 11.1.10-h25, 11.1.13-h5, 11.1.15 PAN-OS 10.2 Versions prior to 10.2.7-h34, 10.2.10-h36, 10.2.13-h21, 10.2.16-h7, 10.2.18-h6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2026-0300

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38821, CVE-2019-10744, CVE-2026-4800, CVE-2025-62718, CVE-2026-25547, CVE-2026-29063, CVE-2026-32871, CVE-2026-39892, CVE-2026-34520, CVE-2026-33937)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Copy Data Management QRadar AI Assistant – Versions 1.0.0 – 1.4.0 Platform Navigator in IBM Cloud Pak for Integration (CP4I) • Versions 16.1.0 to 16.1.0.22, 16.1.1, 16.1.2, 16.1.3.0 to 16.1.3.4 • Versions 4.0.0-sc2 to 4.0.19-sc2, 4.1.0, 4.2.0, 4.3.0, 4.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7232411 • https://www.ibm.com/support/pages/node/7271765 • https://www.ibm.com/support/pages/node/7271726

ffected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-41073, CVE-2025-40252, CVE-2025-68724, CVE-2026-31402, CVE-2026-23401, CVE-2026-31431, CVE-2026-23097, CVE-2026-23193, CVE-2025-71238, CVE-2026-23191)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exists in the kernel of 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	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:13577 • https://access.redhat.com/errata/RHSA-2026:13664 • https://access.redhat.com/errata/RHSA-2026:13681 • https://access.redhat.com/errata/RHSA-2026:13734 • https://access.redhat.com/errata/RHSA-2026:13887

Affected Product	**Juniper Networks**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11083, CVE-2025-39697, CVE-2025-39971, CVE-2025-64720, CVE-2025-65018, CVE-2025-66293, CVE-2025-9086, CVE-2025-12818, CVE-2025-38129, CVE-2025-38248, CVE-2025-40064, CVE-2025-68800, CVE-2025-69419, CVE-2025-71085, CVE-2026-23001, CVE-2026-23074, CVE-2026-23097)
Description	Juniper has released a security update addressing multiple vulnerabilities that exists in their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Juniper Networks Juniper Secure Analytics • From 7.5.0 before 7.5.0 UP15 IF01.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP15-IF01

Affected Product	**cPanel**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23918, CVE-2026-24072, CVE-2026-33006, CVE-2026-28780, CVE-2026-29168, CVE-2026-29169, CVE-2026-33007, CVE-2026-33523, CVE-2026-33857, CVE-2026-34032, CVE-2026-34059, CVE-2026-5545, CVE-2026-4873, CVE-2026-7168, CVE-2026-6253, CVE-2026-6276, CVE-2026-6429)
Description	cPanel has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	EasyApache 25.57 • ea-libcurl: security backports from curl v8.20.0 • ea-apache24 from v2.4.66 to v2.4.67
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Affected Product	**IBM**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22112, CVE-2016-5007, CVE-2022-22978, CVE-2016-9879, CVE-2019-1010266, CVE-2020-28500, CVE-2018-16487, CVE-2018-3721, CVE-2020-8203, CVE-2021-23337, CVE-2026-40175, CVE-2026-25645, CVE-2026-33671, CVE-2026-33672, CVE-2026-34070, CVE-2026-40087, CVE-2026-2950, CVE-2026-4539, CVE-2025-67221, CVE-2025-64340, CVE-2026-27124, CVE-2026-33123, CVE-2026-34073, CVE-2026-22815, CVE-2026-34513, CVE-2026-34514, CVE-2026-34515, CVE-2026-34516, CVE-2026-34517, CVE-2026-34518, CVE-2026-34519, CVE-2026-34525, CVE-2026-0540, CVE-2026-28804, CVE-2026-33938, CVE-2026-33939, CVE-2026-33940, CVE-2026-33941, CVE-2025-68161)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Copy Data Management IBM Db2 • Versions 11.5.0 – 11.5.9 • Versions 12.1.0 – 12.1.4 QRadar AI Assistant – Versions 1.0.0 – 1.4.0 Platform Navigator in IBM Cloud Pak for Integration (CP4I) • Versions 16.1.0 to 16.1.0.22, 16.1.1, 16.1.2, 16.1.3.0 to 16.1.3.4 • 4.0.0-sc2 to 4.0.19-sc2, 4.1.0, 4.2.0, 4.3.0, 4.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7232411 • https://www.ibm.com/support/pages/node/7271765 • https://www.ibm.com/support/pages/node/7271726 • https://www.ibm.com/support/pages/node/7269429

Affected Product	**Dell**
Severity	**Low**
Affected Vulnerability	Insufficient Logging Vulnerability (CVE-2026-32803)
Description	Dell has released a security update addressing a vulnerability that exists in their products. **CVE-2026-32803:** Dell PowerScale OneFS versions 9.5.0.0 through 9.5.1.6, 9.6.0.0 through 9.7.1.13, 9.8.0.0 through 9.10.1.5 and 9.11.0.0 through 9.12.0.1 contains an Insufficient Logging vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerScale Onefs – Versions 9.5.0.0 through 9.5.1.6 PowerScale Onefs – Versions 9.6.0.0 through 9.7.1.13 PowerScale Onefs – Versions 9.8.0.0 through 9.10.1.5 PowerScale Onefs – Versions 9.11.0.0 through 9.12.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000461228/dsa-2026-172-security-update-for-dell-powerscale-onefs-insufficient-logging-vulnerability

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.