Advisory Alert

Alert Number: AAA20260428 **Date:** April 28, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Zyxel Networks	**High**, **Medium**	Command Injection Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-4800, CVE-2026-33186, CVE-2026-29063, CVE-2026-33228)
Description	IBM 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. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar Log Management AQL Plugin versions 1.0.0 to 1.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7270845

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 the affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Disk Library for mainframe DLm8700 versions prior to 7.0.1.0 • Disk Library for mainframe DLm2700 versions prior to 7.0.1.0 • PowerProtect Cyber Recovery 20.1.0.0-22 - Software : cr-release-bundle-20.1.0.0-22.tar.gz • PowerProtect Cyber Recovery 20.1.0.0-22 (OVA): dellemc-cyber-recovery-20.1.0.0-22.ova • PowerProtect Cyber Recovery SLES 15.4 Virtual Appliance OS Security Patch: cyber-recovery-osupdate-15.4.0-14.bin • Dell NativeEdge Orchestrator Version 3.1.0.0 • Dell Automation Platform Versions prior to 2.0.0.0 • APEX Cloud Platform for Red Hat OpenShift Versions prior to 03.04.04.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000458131/dsa-2026-091-security-update-for-dell-disk-library-for-mainframe-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000458096/dsa-2026-155-security-update-for-dell-powerprotect-cyber-recovery-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000458049/dsa-2026-193-security-update-for-dell-automation-platform-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000457936/dsa-2026-194-security-update-for-dell-apex-cloud-platform-for-red-hat-openshift-for-multiple-third-party-component-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23097, CVE-2026-31402, CVE-2025-68741, CVE-2026-23001, CVE-2026-23111)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the 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 9.6 aarch64 and 10.0 aarch64 • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x and 10.0 s390x • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le and 10.0 ppc64le • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 and 10.0 x86_64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 and 10.0 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.6 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 and 10.0 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x and 10.0 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.6 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x and 10.0 s390x • Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le 10.0 ppc64le • Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 and 10.0 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 • Red Hat Enterprise Linux Server - AUS 9.6 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:11313 • https://access.redhat.com/errata/RHSA-2026:10996

Affected Product	**Zyxel Networks**
Severity	**High**, **Medium**
Affected Vulnerability	Command Injection Vulnerabilities (CVE-2026-0711, CVE-2026-1460)
Description	Zyxel has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-0711**: A post-authentication command injection vulnerability in the EasyMesh-related APIs of certain 4G LTE/5G NR CPE, DSL/Ethernet, CPE Fiber ONTs, and Wireless Extenders firmware versions could allow an authenticated, adjacent attacker with administrator privileges to execute OS commands on an affected device. It is important to note that WAN access is disabled by default on these devices, and this attack can only succeed if user-configured passwords have been compromised. **CVE-2026-1460**: A post-authentication command injection vulnerability in the EasyMesh-related APIs of certain 4G LTE/5G NR CPE, DSL/Ethernet, CPE Fiber ONTs, and Wireless Extenders firmware versions could allow an authenticated, adjacent attacker with administrator privileges to execute OS commands on an affected device. It is important to note that WAN access is disabled by default on these devices, and this attack can only succeed if user-configured passwords have been compromised. Zyxel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-and-wireless-extenders-04-28-2026

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2015-8797, CVE-2026-24051, CVE-2026-32141, CVE-2026-2950, CVE-2026-22029, CVE-2025-13465, CVE-2026-33532, CVE-2025-15284, CVE-2025-68470, CVE-2026-2391, CVE-2026-27601, CVE-2025-15599, CVE-2026-0540, CVE-2026-3621, CVE-2025-2099)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Operations Analytics - Log Analysis versions 1.3.2.0, 1.3.3.0, 1.3.5.0, 1.3.5.1 and 1.3.5.2 IBM Security QRadar Log Management AQL Plugin versions 1.0.0 to 1.1.4 IBM Cloud Pak for Applications versions 5.1, 5.2 and 5.3 IBM WebSphere Application Server Liberty versions 17.0.0.3 to 26.0.0.4 DataStage on Cloud Pak for Data versions 5.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7270822 • https://www.ibm.com/support/pages/node/7270845 • https://www.ibm.com/support/pages/node/7270869 • https://www.ibm.com/support/pages/node/7270924

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.