Advisory Alert

Alert Number: AAA20260804 **Date:** August 4, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Zyxel	**High**, **Medium**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-68214, CVE-2026-23199, CVE-2026-52923, CVE-2026-45416, CVE-2026-45674, CVE-2026-50010, CVE-2026-47691, CVE-2026-44249)
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 8 Base & CodeReady Builder: x86_64, aarch64, ppc64le, s390x • Red Hat Enterprise Linux 8.10 Extended Life Cycle: x86_64, aarch64, ppc64le, s390x • Red Hat Enterprise Linux 10 Base & CodeReady Builder: x86_64, aarch64, ppc64le, s390x • Red Hat Enterprise Linux 10.2 Extended Update Support & CodeReady EUS: x86_64, aarch64, ppc64le, s390x • Red Hat Enterprise Linux 10.2 Four Years of Updates: x86_64, aarch64, ppc64le, s390x • Red Hat Enterprise Linux 10.2 Extended Life Cycle: x86_64, aarch64, ppc64le, s390x • JBoss Enterprise Application Platform Text-Only Advisories: x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:49871 https://access.redhat.com/errata/RHSA-2026:49857 https://access.redhat.com/errata/RHSA-2026:49701

Vendor	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-56793, CVE-2026-56794, CVE-2026-40717, CVE-2026-64993)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000494958/dsa-2026-326-security-update-for-dell-openmanage-server-administrator-omsa-network-access-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000481265/dsa-2026-295 • https://www.dell.com/support/kbdoc/en-us/000494748/dsa-2026-325-security-update-for-dell-rvtools-vulnerability

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-10025, CVE-2026-13477, CVE-2026-21945, CVE-2026-21932, CVE-2026-21933, CVE-2026-21925)
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	QRadar versions: • 7.6.0.0 to 7.6.0.1 • 7.5.0 to 7.5.0 UP 15 IF05 IBM Storage Protect for VMs: Data Protection for VMware versions 8.1.0.0 to 8.2.1.0 IBM Storage Protect for VMs: Data Protection for Hyper-V versions 8.1.0.0 to 8.2.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7282394 https://www.ibm.com/support/pages/node/7282395 https://www.ibm.com/support/pages/node/7282313

Vendor	**Zyxel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-14818, CVE-2026-6837, CVE-2026-8508)
Description	Zyxel has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-14818:** A path traversal vulnerability in the CLI command used to execute configuration files in certain versions of ZLD firewall firmware could allow an authenticated attacker with administrator privileges to execute a crafted malicious configuration file on an affected device. **CVE-2026-6837:** A post-authentication command injection vulnerability in the "export-cgi" CGI program in certain AP firmware versions could allow an authenticated attacker with administrator privileges to execute OS commands on an affected device. **CVE-2026-8508:** An improper authentication vulnerability in the "social_login.cgi" CGI program in certain firmware versions of APs, FWA7, and Security Routers could allow an attacker on the WLAN to bypass captive portal authentication. Zyxel advises to apply security fixes at your earliest to protect 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-path-traversal-vulnerability-in-the-configuration-file-execution-cli-command-of-zld-firewalls-08-04-2026 • https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-improper-authentication-vulnerabilities-in-certain-aps-fwa7-and-security-routers-08-04-2026

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.