Advisory Alert

Alert Number: AAA20260918 **Date:** September 18, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-5222, CVE-2026-1933, CVE-2026-2340, CVE-2026-3012, CVE-2026-3833, CVE-2026-4408, CVE-2026-6893, CVE-2026-11822, CVE-2026-11824, CVE-2026-14164, CVE-2026-15816, CVE-2026-29111, CVE-2026-33845, CVE-2026-33846, CVE-2026-34982, CVE-2026-41411, CVE-2026-42009, CVE-2026-42010, CVE-2026-43112, CVE-2026-48864, CVE-2025-68121, CVE-2026-15809, CVE-2026-25679, CVE-2026-32280, CVE-2026-34986, CVE-2026-39820, CVE-2026-42499, CVE-2026-16313, CVE-2026-1519, CVE-2026-3039, CVE-2026-5946, CVE-2026-10723, CVE-2026-11331, CVE-2026-13321, CVE-2026-39821, CVE-2024-58007, CVE-2026-23172, CVE-2026-52971, CVE-2026-53176, CVE-2026-53192, CVE-2026-53193, CVE-2026-63869, CVE-2026-63923, CVE-2026-64029, CVE-2026-64175, CVE-2026-64176, CVE-2026-64414, CVE-2026-64456, CVE-2026-68128, CVE-2026-68143, CVE-2026-68200, CVE-2026-68294, CVE-2026-68363, CVE-2026-72102)
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 Platform & Enterprise Software: • Red Hat OpenShift Container Platform 4.12, 4.13 & 4.18 (RHEL 8 / 9) across aarch64, ppc64le, s390x, and x86_64 architectures. • Red Hat Enterprise Linux 10 Base and CodeReady Linux Builder across aarch64, ppc64le, s390x, and x86_64 architectures. • Red Hat Enterprise Linux 10.2 4 Years of Updates / Support, Extended Life Cycle, Extended Update Support (EUS), and CodeReady Linux Builder (Extended Update Support) across aarch64, ppc64le, s390x, and x86_64 architectures.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:68507 https://access.redhat.com/errata/RHSA-2026:65851 https://access.redhat.com/errata/RHSA-2026:66385 https://access.redhat.com/errata/RHSA-2026:65907 https://access.redhat.com/errata/RHSA-2026:65906 https://access.redhat.com/errata/RHSA-2026:65838 https://access.redhat.com/errata/RHSA-2026:65839

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
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: 15.4, 15.5, 15.6 SUSE Linux Enterprise 12 SP5: High Performance Computing, Live Patching, Server, Server for SAP Applications SUSE Linux Enterprise 15 (SP4, SP5, SP6, SP7): • Modules (SP7): Basesystem, Development Tools, Legacy, Public Cloud • Desktop / Workstation (SP7): SLED 15 SP7, Workstation Extension • High Availability Extension: SP7 • High Performance Computing: SP4, SP5 • Live Patching: SP4, SP5, SP6, SP7 • Real Time: SP4, SP5, SP6, SP7 • Server / SAP Applications: SP4, SP5, SP6, SP7 SUSE Linux Enterprise Micro: 5.3, 5.4, 5.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264254-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264224-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264231-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264244-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264243-1/

Vendor	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-81469, CVE-2026-82165, CVE-2026-49810)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-81469:** Dell Inventory Collector Client, versions prior to 15.0.0, contain an Unquoted Search Path or Element vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution and Elevation of Privileges **CVE-2026-82165:** Dell Command | Integration Suite for System Center, versions prior to 6.7.2, contain an Incorrect Default Permissions vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information Disclosure. **CVE-2026-49810:** Dell Command Powershell Provider (DCPP), versions prior to 2.10.2 contain an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information Disclosure. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Inventory Collector versions prior to 15.0.0 Dell Command | Integration Suite for Microsoft System Center versions Prior to 6.7.2 Dell Command | PowerShell Provider (DCPP) versions prior to 2.10.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000502474/dsa-2026-381-security-update-for-dell-supportassist-for-pcs-home-and-business-dell-optimizer-dell-trusted-device-dell-command-update-for-an-unquoted-search-path-or-element-vulnerability • https://www.dell.com/support/kbdoc/en-us/000506922/dsa-2026-409-security-update-for-dell-command-integration-suite-for-system-center-for-an-incorrect-default-permissions-vulnerability • https://www.dell.com/support/kbdoc/en-us/000502472/dsa-2026-379-security-update-for-dell-command-powershell-provider-dcpp-for-a-credential-theft-via-powershell-event-log-vulnerability

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-45819, CVE-2026-73088, CVE-2026-73089, CVE-2026-45409, CVE-2026-49477, CVE-2026-49476, CVE-2026-69249, CVE-2026-69248, CVE-2026-69247)
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 Security SOAR: 51.0.6 – 51.0.11 IBM SOAR QRadar Plugin App: 5.3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7287953 https://www.ibm.com/support/pages/node/7287954 https://www.ibm.com/support/pages/node/7287955 https://www.ibm.com/support/pages/node/7287956 https://www.ibm.com/support/pages/node/7287958

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.