Advisory Alert

Alert Number: AAA20260805 **Date:** August 5, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Multiple Vulnerabilities
Veeam	**Critical**	Multiple Vulnerabilities
Check Point	**High**	Authentication Bypass Vulnerability
Veeam	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Lenovo	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-14529, CVE-2026-14446, CVE-2026-14512, CVE-2026-33896, CVE-2026-27606, CVE-2026-1615, CVE-2025-61140, CVE-2026-48714)
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 Cloud Pak System - Version 2.3.5.0 IBM WebSphere Hybrid Edition 5.1 IBM WebSphere Application Server Versions • 9.0.0.0 - 9.0.5.28 • 8.5.5.0 - 8.5.5.29 IBM WebSphere Application Server Liberty - Versions 17.0.0.3 - 26.0.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7282517 • https://www.ibm.com/support/pages/node/7282447 • https://www.ibm.com/support/pages/node/7282495 • https://www.ibm.com/support/pages/node/7282496

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-63455, CVE-2026-63456)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-63455:** Multiple vulnerabilities in the REST API interface of HPE Networking SD-WAN Orchestrator could allow an unauthenticated remote attacker to bypass web authentication mechanisms and access system functions. Successful exploitation could allow an attacker to view and modify potentially sensitive information on the target system. **CVE-2026-63456:** Multiple vulnerabilities in the REST API interface of HPE Networking SD-WAN Orchestrator could allow an unauthenticated remote attacker to bypass web authentication mechanisms and access system functions. Successful exploitation could allow an attacker to view and modify potentially sensitive information on the target system. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking SD-WAN Orchestrator • SD-WAN Orchestrator 9.6.2.x: 9.6.2.40208 and below • SD-WAN Orchestrator 9.6.3.x: 9.6.3.40137 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05100en_us&docLocale=en_US

Vendor	**Veeam**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-58073, CVE-2026-58072)
Description	Veeam has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-58073:** A vulnerability in Veeam Service Provider Console allowing an unauthenticated attacker to impersonate a managed agent and obtain that agent's credentials. **CVE-2026-58072:** A vulnerability in Veeam Service Provider Console allowing arbitrary file write on the management server, which can lead to remote code execution. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Service Provider Console 9.3.0.35057 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4893

Vendor	**Check Point**
Severity	**High**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-18574)
Description	Check Point has released a security update addressing a vulnerability that exists in their products. **CVE-2026-18574:** An unauthenticated attacker may be able to bypass Management authentication and execute arbitrary commands on the Security Management Server. Successful exploitation could result in full compromise of the Security Management system. Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Security Management Server, Multi-Domain Security Management Server (MDS) Versions R80, R80.10, R80.20, R80.30, R80.40, R81, R81.10 (all EoS) R81.20, R82, R82.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk185222

Vendor	**Veeam**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-58067, CVE-2026-58071)
Description	Veeam has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-58067:** A vulnerability in Veeam Service Provider Console allowing an unauthenticated attacker to exhaust host memory and cause a denial of service. **CVE-2026-58071:** A vulnerability in Veeam Service Provider Console allowing an unauthenticated attacker to access the proxied appliance API as Portal Administrator during a short window after an administrator session begins. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Service Provider Console 9.3.0.35057 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4893

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-48059, CVE-2026-47691, CVE-2026-50560, CVE-2026-50011, CVE-2026-44250, CVE-2026-44890, CVE-2026-44249, CVE-2026-50020, CVE-2026-44893, CVE-2026-50010, CVE-2026-45673, CVE-2026-45416, CVE-2026-45536, CVE-2026-45674, CVE-2026-46340, CVE-2026-47244, CVE-2026-48006, CVE-2026-48043, CVE-2026-42587, CVE-2026-52923, CVE-2025-68214, CVE-2026-23199)
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 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 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 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-2026:49857 • https://access.redhat.com/errata/RHSA-2026:49871 • https://access.redhat.com/errata/RHSA-2026:50085

Vendor	**Lenovo**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-16791, CVE-2026-16792, CVE-2026-16793)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-16791:** A temporary file creation vulnerability in the Linux version of Lenovo XClarity Essentials OneCLI 5.5.0 and below could allow a local low-privileged attacker to overwrite or truncate arbitrary local files with program-generated data when OneCLI is executed with elevated privileges. **CVE-2026-16792:** An improper certificate validation vulnerability was reported in multiple Lenovo XClarity Orchestrator (LXCO) 2.2.0 microservices that could allow an adjacent network attacker to intercept sensitive communications by performing a machine-in-the-middle attack against HTTPS connections during TLS certificate validation under certain circumstances. **CVE-2026-16793:** An improper neutralization of special elements used in an operating system command vulnerability was reported in Lenovo XClarity Orchestrator (LXCO) 2.2.0 that could allow an authenticated attacker to execute arbitrary operating system commands as a privileged user under a specific circumstance. Lenovo 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://support.lenovo.com/us/en/product_security/LEN-216074 • https://support.lenovo.com/us/en/product_security/LEN-216072

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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 these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak System - Version 2.3.5.0 IBM WebSphere Hybrid Edition 5.1 IBM WebSphere Application Server Versions • 8.5 & 9.0 • 9.0.0.0 - 9.0.5.28 • 8.5.5.0 - 8.5.5.29 IBM WebSphere Application Server Liberty - Versions 17.0.0.3 - 26.0.0.8 & Continuous delivery PowerVC Versions: • 2.3.0 • 2.3.1 • 2.3.2 • 2.3.3 IBM Db2 Bridge All Versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/

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.