



Advisory Alert

Alert Number: **AAA20261007** Date: October 7, 2026

Document Classification Level : **Public Circulation Permitted | Public**

Information Classification Level : **TLP: WHITE**

Overview

Vendor	Severity	Vulnerability
Veeam	Critical	Remote Code Execution Vulnerability
HPE	Critical	Multiple Vulnerabilities
SonicWall	Critical	Multiple Vulnerabilities
Dell	Critical	Multiple Vulnerabilities
IBM	Critical	Multiple Vulnerabilities
Red Hat	High	Multiple Vulnerabilities
SUSE	High	Multiple Vulnerabilities
HPE	High, Medium	Multiple Vulnerabilities
Apache Struts	High, Medium	Multiple Vulnerabilities
Ubuntu	High, Medium, Low	Multiple Vulnerabilities
IBM	High, Medium, Low	Multiple Vulnerabilities
Veeam	Medium	Multiple Vulnerabilities
MongoDB	Low	Improper Validation Vulnerability

Description

Vendor	Veeam
Severity	Critical
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-64393)
Description	Veeam has released a security update addressing a vulnerability that exists in their products. CVE-2025-64393: A vulnerability allowing a low-privileged user with the Backup Viewer role to perform remote code execution (RCE) on the Veeam Backup Server through insecure deserialization of untrusted data received via the Mount Service. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication 12.3.2.4854 and all earlier version 12 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4934

Vendor	HPE
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76742, CVE-2026-76743, CVE-2026-76744, CVE-2026-76745, CVE-2026-76746, CVE-2026-76747, CVE-2026-79798, CVE-2026-76750, CVE-2026-76751, CVE-2026-76752, CVE-2026-76753, CVE-2026-76754, CVE-2026-79796, CVE-2026-79801, CVE-2026-79805, CVE-2026-79794)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE Networking AOS-Switch (AOS-S): - AOS-S 16.11.0031 and below HPE Networking ClearPass Policy Manager (CPPM): - CPPM 6.14.0 and below - CPPM 6.11.15 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05156en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05158en_us&docLocale=en_US

Vendor	SonicWall
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-102255, CVE-2026-102256, CVE-2026-102257, CVE-2026-102258)
Description	SonicWall 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. SonicWall advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SMA1000 Models - 6210, 7210, 8200v: 12.4.3-03526 (platform-hotfix) and older versions 12.5.0-02952 (platform-hotfix) and older versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0017

Vendor	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 these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SmartFabric Storage Software Versions prior to 1.4.6 Vapp Software versions prior to 6.1.1.1: - Dell Storage Resource Manager - Dell Storage Monitoring and Reporting
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000517986/dsa-2026-443-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000517934/dsa-2026-457-security-update-for-dell-networking-smartfabric-storage-software-vulnerabilities

Vendor	IBM
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-58062, CVE-2026-59650, CVE-2026-8763)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. CVE-2026-58062: In Bouncy Castle for Java before 1.85, Stapled OCSP response accepted without binding to the checked certificate. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series). CVE-2026-59650: In Bouncy Castle for Java before 1.85, MTI/A0 DH agreement exponentiates unvalidated peer value. This issue also affects Bouncy Castle for Java LTS before 2.73.12. CVE-2026-8763: In Bouncy Castle for Java before 1.85, Name Constraints bypass via trailing dot in rfc822Name and URI. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 1.0.2.7 (1.0.X series), 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series). IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Cloud Object Storage System versions: 3.8.1.54 to 3.19.5.56 3.20.0.0 to 3.20.0.97
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7291384

Vendor	SUSE
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46116, CVE-2026-63888, CVE-2026-63920, CVE-2026-64011, CVE-2026-64114, CVE-2026-68121, CVE-2026-68202, CVE-2026-63802, CVE-2026-63912, CVE-2026-63917, CVE-2026-63921, CVE-2026-63944, CVE-2026-63971, CVE-2026-63994, CVE-2026-64000, CVE-2026-64121, CVE-2026-64189, CVE-2026-74394, CVE-2026-74612)
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 - Leap 15.6 - Leap 15.4 SUSE Linux Enterprise 15 Series Service Pack 7 (SP7) - Live Patching - Real Time - Server (SLES) - Server for SAP Applications Service Pack 6 (SP6) - Live Patching - Real Time - Server (SLES) - Server for SAP Applications Service Pack 4 (SP4) - High Performance Computing (HPC) - Live Patching - Real Time - Server (SLES) - Server for SAP Applications SUSE Linux Enterprise 12 Series Service Pack 5 (SP5) - High Performance Computing (HPC) - Live Patching - Server (SLES) - Server for SAP Applications SUSE Linux Enterprise Micro - SLE Micro 5.4 - SLE Micro 5.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264550-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264548-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264542-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264530-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264540-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264518-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264538-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264537-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264536-1/

Vendor	Red Hat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31663, CVE-2026-31581, CVE-2026-45984, CVE-2026-45991, CVE-2026-46043, CVE-2026-46133, CVE-2026-52924, CVE-2026-53239, CVE-2026-64007, CVE-2026-63921, CVE-2026-63919, CVE-2026-63917, CVE-2026-64582, CVE-2026-68294, CVE-2026-68426, CVE-2026-74556, CVE-2026-74746, CVE-2026-80864, CVE-2026-80863, CVE-2025-68347, CVE-2026-52923, CVE-2026-53062, CVE-2026-64320, CVE-2026-68480, CVE-2026-33814, CVE-2026-74469, CVE-2026-80844, CVE-2026-81000, CVE-2026-39829, CVE-2026-63385, CVE-2026-81634, CVE-2026-82717, CVE-2026-89846)
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	OpenShift Container Platform OpenShift Container Platform 4.22: - RHEL 9 Base (aarch64, ppc64le, s390x, x86_64) - RHEL 8 Base (aarch64, ppc64le, s390x, x86_64) OpenShift Container Platform 4.21: - RHEL 9 Base (aarch64, ppc64le, s390x, x86_64) - RHEL 8 Base (aarch64, ppc64le, s390x, x86_64) OpenShift Container Platform 4.20: - RHEL 9 Base (aarch64, ppc64le, s390x, x86_64) - RHEL 8 Base (aarch64, ppc64le, s390x, x86_64) RHEL 8.6: - Advanced Update Support (AUS) (x86_64) - Extended Life Cycle Long Life (aarch64, ppc64le, s390x, x86_64) RHEL 8.4: - Advanced Update Support (AUS) (x86_64) - Extended Life Cycle Long Life (aarch64, ppc64le, s390x, x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:77217 https://access.redhat.com/errata/RHSA-2026:77216 https://access.redhat.com/errata/RHSA-2026:74376 https://access.redhat.com/errata/RHSA-2026:74377 https://access.redhat.com/errata/RHSA-2026:76979 https://access.redhat.com/errata/RHSA-2026:76814 https://access.redhat.com/errata/RHSA-2026:74428 https://access.redhat.com/errata/RHSA-2026:74379

Vendor	HPE
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76748, CVE-2026-76741, CVE-2026-76749, CVE-2026-79797, CVE-2026-79799, CVE-2026-79800, CVE-2026-79802, CVE-2026-79803, CVE-2026-79806, CVE-2026-79807, CVE-2026-79808, CVE-2026-79809, CVE-2026-79810, CVE-2026-79811, CVE-2026-79814, CVE-2026-79813, CVE-2026-79815, CVE-2026-79812, CVE-2026-79817, CVE-2026-79816, CVE-2026-79818)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE Networking AOS-Switch (AOS-S): - AOS-S 16.11.0031 and below HPE Networking ClearPass Policy Manager (CPPM): - CPPM 6.14.0 and below - CPPM 6.11.15 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05156en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05158en_us&docLocale=en_US

Vendor	Apache Struts
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-104711, CVE-2026-104712, CVE-2026-104713, CVE-2026-104714)
Description	Apache Struts 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. Apache Struts advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Struts 2.0.0 through Struts 2.3.37 (EOL) Struts 2.5.0 through Struts 2.5.33 (EOL) Struts 6.0.0 through Struts 6.11.0 Struts 7.0.0 through Struts 7.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://cwiki.apache.org/confluence/spaces/WW/pages/446070946/S2-075 https://cwiki.apache.org/confluence/spaces/WW/pages/446071762/S2-076 https://cwiki.apache.org/confluence/spaces/WW/pages/451972213/S2-077 https://cwiki.apache.org/confluence/spaces/WW/pages/451972217/S2-078

Vendor	Ubuntu
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 20.04, 22.04, 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8887-1 https://ubuntu.com/security/notices/USN-8875-1 https://ubuntu.com/security/notices/USN-8879-1 https://ubuntu.com/security/notices/USN-8878-1 https://ubuntu.com/security/notices/USN-8876-1

Vendor	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27775, CVE-2022-27776, CVE-2024-23556, CVE-2024-0853, CVE-2024-42200, CVE-2024-42189, CVE-2024-42193, CVE-2023-37520, CVE-2024-13176, CVE-2025-9086, CVE-2026-19032, CVE-2026-83557, CVE-2026-56864, CVE-2026-56865, CVE-2025-71329, CVE-2025-71330, CVE-2026-12185, CVE-2026-12803, CVE-2026-12816, CVE-2026-12860, CVE-2026-13506, CVE-2026-13586, CVE-2026-14682, CVE-2026-15055, CVE-2026-58059, CVE-2026-58060, CVE-2026-58061, CVE-2026-58063, CVE-2026-59647, CVE-2026-59648, CVE-2026-59651, CVE-2026-59652, CVE-2026-12802, CVE-2026-59639, CVE-2026-59642, CVE-2026-59884, CVE-2026-59885, CVE-2026-59886, CVE-2026-44405, CVE-2026-44307, CVE-2026-59890, CVE-2025-5115)
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 2.3.5.0 and 2.3.6.0 IBM Cloud Object Storage System versions: 3.8.1.54 to 3.19.5.56 3.20.0.0 to 3.20.0.97
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7276505 https://www.ibm.com/support/pages/node/7291384

Vendor	Veeam
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-93026, CVE-2025-64392)
Description	Veeam 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. Veeam advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Veeam Backup & Replication 12.3.2.4854 and all earlier version 12 builds. Veeam Backup Enterprise Manager (Veeam Backup & Replication) 12.3.2.4854 and all earlier version 12 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4934

Vendor	MongoDB
Severity	Low
Affected Vulnerability	Improper Validation Vulnerability (CVE-2026-103546)
Description	MongoDB has released a security update addressing a vulnerability that exists in their products. CVE-2026-103546: In MongoDB Controllers for Kubernetes, insufficient validation of Ops Manager backup configuration may allow a user who can modify an OpsManager custom resource to cause unintended administrative changes in Ops Manager. This affects deployments using Enterprise Ops Manager backup reconciliation. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Mongodb Controllers for Kubernetes versions prior to 1.13.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

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.