Advisory Alert

Alert Number: AAA20261030 **Date:** October 30, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Veeam	**Critical**	Remote Code Execution Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Veeam	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
MongoDB	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-8633, CVE-2026-9319, CVE-2026-14529, CVE-2026-14525, CVE-2026-14512, CVE-2026-8644, CVE-2026-11712, CVE-2026-11708, CVE-2026-9330, CVE-2026-9311, CVE-2026-11707, CVE-2026-14446)
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 Security Verify Directory Versions - 10.0.0-10.0.4 IBM Verify Directory Versions - 11.0.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7294603

Vendor	**Veeam**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2023-22793)
Description	Veeam has released a security update addressing a vulnerability that exists in their products. **CVE-2023-22793:** A vulnerability allowing an unauthenticated attacker to perform remote code execution (RCE) on servers running the Veeam Virtualization Extensions service of Veeam Management Pack for Microsoft System Center. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Management Pack for Microsoft System Center 9.1 and all earlier version 9 builds, including the Veeam Backup & Replication 13 compatibility patch.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4961

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53266, CVE-2026-68121, CVE-2026-74480, CVE-2026-74582, CVE-2026-80844, CVE-2026-72288, CVE-2026-72289, CVE-2026-90011, CVE-2026-98222, CVE-2026-43051, CVE-2026-53073, CVE-2026-53224, CVE-2026-53246)
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 Server - AUS Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle Red Hat Enterprise Linux for x86_64 Red Hat Enterprise Linux for IBM z Systems Red Hat Enterprise Linux for Power, little endian Red Hat Enterprise Linux for ARM 64 Red Hat CodeReady Linux Builder for x86_64 Red Hat CodeReady Linux Builder for Power, little endian Red Hat CodeReady Linux Builder for ARM 64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle Red Hat Enterprise Linux for x86_64 - Extended Update Support Red Hat Enterprise Linux for IBM z Systems - Extended Update Support Red Hat Enterprise Linux for Power, little endian - Extended Update Support Red Hat Enterprise Linux for ARM 64 - Extended Update Support Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support Red Hat Enterprise Linux for ARM 64 - 4 years of updates Red Hat Enterprise Linux for IBM z Systems - 4 years of updates Red Hat Enterprise Linux for Power, little endian - 4 years of support Red Hat Enterprise Linux for x86_64 - 4 years of updates
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:92629 https://access.redhat.com/errata/RHSA-2026:92209 https://access.redhat.com/errata/RHSA-2026:92362

Vendor	**Veeam**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-107239, CVE-2026-107238)
Description	Veeam has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-107239:** A vulnerability allowing a member of the Veeam Virtualization Extensions Users group to perform remote code execution (RCE) on servers running the Veeam Management Pack for Microsoft System Center Collector service. **CVE-2026-107238:** A vulnerability allowing an authenticated domain user to perform remote code execution (RCE) as the LocalSystem account on servers running the Veeam Management Pack for Microsoft System Center Collector service. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Management Pack for Microsoft System Center 9.1 and all earlier version 9 builds, including the Veeam Backup & Replication 13 compatibility patch.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4961

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	• SUSE Linux Enterprise 11 SP4: Server, Server LTSS EXTREME CORE • openSUSE Leap: 15.4, 15.5, 15.6 • SUSE Linux Enterprise 15 SP4: High Availability Extension, High Performance Computing, High Performance Computing ESPOS, High Performance Computing LTSS, Live Patching, Real Time, Server, Server LTSS, Server for SAP Applications • SUSE Linux Enterprise 15 SP5: High Performance Computing, High Performance Computing ESPOS, High Performance Computing LTSS, Live Patching, Real Time, Server, Server LTSS, Server for SAP Applications • SUSE Linux Enterprise 15 SP6: High Availability Extension, Live Patching, Real Time, Server, Server LTSS, Server for SAP Applications • SUSE Linux Enterprise 15 SP7: Basesystem Module, Development Tools Module, Legacy Module, Public Cloud Module, Real Time Module, Desktop, High Availability Extension, Live Patching, Real Time, Server, Server for SAP Applications, Workstation Extension • SUSE Linux Enterprise Micro: 5.3, 5.4, 5.5 • SUSE Linux Enterprise Micro for Rancher: 5.3, 5.4 • SUSE Manager 4.3: Proxy, Retail Branch Server, Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264933-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264934-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264935-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264936-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264937-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264938-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264939-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264940-1/

Vendor	**MongoDB**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-116641, CVE-2026-118581, CVE-2026-118510)
Description	MongoDB has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-116641:** The DB Tools rely on the TLS implementation in Golang's standard library, which generally uses the system CA store. However, the crypto/x509 package also has its own internal denylist of known-bad CA certificates. Golang 1.27.3 adds the eMudhra certificates to this list. DB Tools version 100.19.0 was compiled with Golang 1.26.8, which does not include this check. **CVE-2026-118581:** The MongoDB Java Driver's BSON encoder doesn't check that a raw document's declared length matches the byte range supplied before copying it into an outgoing command. If an application wraps untrusted bytes in such a document, the resulting message can be malformed, and the database may parse attacker-controlled trailing bytes as extra fields of the surrounding command. No authentication or user interaction is needed beyond influencing those bytes through the application. The command that actually runs is altered, which can change the data read or written under the application's credentials. **CVE-2026-118510:** A type-handling flaw in the relationship query building of this MongoDB integration library can cause a check for the absence of a related record to be compiled with an identifier of the wrong data type. In an application that relies on such a check to decide which documents a request may see or act on, a user with basic privileges may be served, may change, or may remove documents that the check was intended to withhold. The failure is silent and produces no error. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Database Tools Versions prior to 100.20.0 • Java Drive 5.8.0 affects versions prior to 5.14.0 • Laravel MongoDB 3.2.3 affects versions prior to 5.12.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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 Verify Directory Versions - 10.0.0-10.0.4 • IBM Verify Directory Versions - 11.0.0.0 • IBM Verify Identity Access Container Versions - 11.0 - 11.0.3.2 • IBM Security Verify Access Container Versions - 10.0 - 10.0.9.4 • IBM Verify Identity Access Versions - 11.0 - 11.0.3.2 • IBM Security Verify Access Versions - 10.0 - 10.0.9.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7294826 https://www.ibm.com/support/pages/node/7294603 https://www.ibm.com/support/pages/node/7294826

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.