Advisory Alert

Alert Number: AAA20260814 **Date:** August 14, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
MongoDB	**Critical**	Integer Overflow Vulnerability
Red Hat	**High**	Use-After-Free Vulnerability
MongoDB	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
PostgreSQL	**High, Medium**	Multiple Vulnerabilities
Ubuntu	**High, Medium, Low**	Multiple Vulnerabilities
OpenSSL	**Low**	Uncontrolled Resource Consumption Vulnerability

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-28808, CVE-2026-42584, CVE-2026-42581, CVE-2026-2332)
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	PowerVC Versions: • 2.3.1 • 2.3.2 • 2.3.3 IBM Storage Scale - Versions 5.2.3.0 - 5.2.3.8 IBM Storage Scale - Versions 6.0.0.0 - 6.0.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7283593 • https://www.ibm.com/support/pages/node/7283638 • https://www.ibm.com/support/pages/node/7283637

Vendor	**MongoDB**
Severity	**Critical**
Affected Vulnerability	Integer Overflow Vulnerability (CVE-2026-19001)
Description	MongoDB has released a security update addressing a vulnerability that exists in their products. **CVE-2026-19001:** The MongoDB BI Connector ODBC Driver may write outside the bounds of a fixed-size buffer when an application supplies an unusually long catalog, schema, or object name to a metadata retrieval function. This may result in memory corruption within the calling application's process, leading to abnormal termination and, under certain conditions, the potential for arbitrary code execution. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BI Connector ODBC Driver - 1.0.0 affects versions prior to 1.4.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://github.com/mongodb/mongo-bi-connector-odbc-driver/releases/tag/v1.4.9

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Use-After-Free Vulnerability (CVE-2026-53264)
Description	Red Hat has released security updates addressing a vulnerability that exists in their products. **CVE-2026-53264:** A flaw was found in the Linux kernel's networking scheduler. A race condition, which is a problem that occurs when multiple operations try to access the same resource at the same time, exists when network filter operations are run concurrently. This can lead to a Use-After-Free (UAF) vulnerability, where the system attempts to use memory that has already been released. This could potentially allow an attacker to cause system instability or execute arbitrary code. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:54482 • https://access.redhat.com/errata/RHSA-2026:54515

Vendor	**MongoDB**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-19502, CVE-2026-19503, CVE-2026-19002, CVE-2026-18888, CVE-2026-19004, CVE-2026-19003)
Description	MongoDB 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. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	BI Connector ODBC Driver - Versions 1.0.0 affects versions prior to 1.4.9 Atlas SQL ODBC Driver - Versions 1.0.0 affects versions prior to 2.0.9 Schema Builder CLI - Versions 1.0.1 affects versions prior to 1.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-41417, CVE-2026-42580, CVE-2026-42585, CVE-2026-42587, CVE-2026-33558, CVE-2026-33870, CVE-2025-11143)
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 Storage Scale - Versions 5.2.3.0 - 5.2.3.8 IBM Storage Scale - Versions 6.0.0.0 - 6.0.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7283638 • https://www.ibm.com/support/pages/node/7283637

Vendor	**PostgreSQL**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-19385, CVE-2026-18408, CVE-2026-18024, CVE-2026-16241, CVE-2026-16239, CVE-2026-16238, CVE-2026-15742, CVE-2026-15741, CVE-2026-14681, CVE-2026-14680, CVE-2026-14679, CVE-2026-14678, CVE-2026-14677, CVE-2026-14676, CVE-2026-14673, CVE-2026-14672, CVE-2026-14671, CVE-2026-14670, CVE-2026-14669, CVE-2026-14668, CVE-2026-14666, CVE-2026-14664, CVE-2026-14663, CVE-2026-14662)
Description	PostgreSQL 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. PostgreSQL advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PostgreSQL Core Server, Clent & Contrib Module Versions: • 18.5 • 17.11 • 16.15 • 15.19 • 14.24
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/support/security/

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	16.04, 22.04, 24.04, 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8630-2 • https://ubuntu.com/security/notices/USN-8631-2 • https://ubuntu.com/security/notices/USN-8637-1 • https://ubuntu.com/security/notices/USN-8530-2 • https://ubuntu.com/security/notices/USN-8548-2 • https://ubuntu.com/security/notices/USN-8529-2 • https://ubuntu.com/security/notices/USN-8633-2

Vendor	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Uncontrolled Resource Consumption Vulnerability (CVE-2026-14456)
Description	OpenSSL has released a security update addressing a vulnerability that exists in their products. **CVE-2026-14456:** A remote peer that can make many Initial packets reach the server listener faster than the application accepts connections, can cause the memory allocated to store the per-channel state to grow without any limits, potentially making the QUIC listener unavailable and causing Denial of Service. OpenSSL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSSL Versions: • from 4.0.0 before 4.0.2 • from 3.6.0 before 3.6.4 • from 3.5.0 before 3.5.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/vulnerabilities/#CVE-2026-14456

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.