Advisory Alert

Alert Number: AAA20260921 **Date:** September 21, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
MongoDB	**Critical**	Multiple Vulnerabilities
Synology	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Improper Access Control Vulnerability
MongoDB	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**MongoDB**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-93762, CVE-2026-93393)
Description	MongoDB has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-93762:** Mongoid contains an unsafe reflection weakness in the query path used for embedded documents. An application that passes an externally supplied field name to certain in-memory query methods may allow an unauthenticated party to obtain unintended disclosure of stored document data and to permanently remove stored records. **CVE-2026-93393:** A heap-based buffer overflow exists in the TLS transport layer of the MongoDB C Driver when built with the Windows platform TLS backend. A remote endpoint that the client connects to, or an attacker able to impersonate or redirect the client's connection, can cause the driver to write attacker-supplied data outside the bounds of a heap allocation while processing incoming encrypted traffic. No authentication or user interaction is required, because the affected processing occurs before any application-level authentication completes. Successful exploitation may lead to memory corruption in the client process, disclosure of adjacent heap memory, or termination of the process. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	C Driver: • 2.4.0 • 2.3.0 affects 2.3.3 and prior versions • 2.2.0 affects 2.2.4 and prior versions • 2.1.0 affects 2.1.2 and prior versions • 2.0.0 affects 2.0.2 and prior versions • 1.30.0 affects 1.30.8 and prior versions • 1.29.0 affects 1.29.2 and prior versions • 1.28.0 affects 1.28.1 and prior versions • 1.27.0 affects 1.27.6 and prior versions • 1.26.0 affects 1.26.2 and prior versions • 1.25.0 affects 1.25.4 and prior versions • 1.24.0 affects 1.24.4 and prior versions Mongoid: • 9.1.0 • 9.0.0 affects 9.0.11 and prior versions • 8.1.0 affects 8.1.12 and prior versions • 8.0.0 affects 8.0.12 and prior versions • 7.6.0 affects 7.6.1 and prior versions • 7.5.0 affects 7.5.4 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Vendor	**Synology**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-13684, CVE-2026-13639, CVE-2026-13635, CVE-2026-13673, CVE-2026-6205, CVE-2026-13666, CVE-2026-13623, CVE-2026-13683)
Description	Synology 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. Synology advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	DSM 7.4 prior to version 7.4-90075 DSM 7.3 prior to version 7.3.2-86009-4 DSM 7.2.2 prior to version 7.2.2-72806-9 DSM 7.2.1 prior to version 7.2.1-69057-12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_26_13

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46117, CVE-2026-53002, CVE-2026-53009, CVE-2026-53185, CVE-2026-63887, CVE-2026-63888, CVE-2026-63952, CVE-2026-64382, CVE-2026-64564, CVE-2026-68166)
Description	Red Hat 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. 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 Enterprise Linux 10.0 • 4 Years of Updates / Support (aarch64, ppc64le, s390x, x86_64) • CodeReady Linux Builder - Extended Update Support (aarch64, ppc64le, s390x, x86_64) • Extended Update Support (EUS) (aarch64, ppc64le, s390x, x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:69089

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2026-49811)
Description	Dell has released a security update addressing a vulnerability that exists in their products. **CVE-2026-49811:** Dell Command | Monitor (DCM), versions prior to 10.13.2, contain an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Command Monitor Software Versions Prior to 10.13.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000502473/dsa-2026-380-security-update-for-dell-command-monitor-dcm-for-an-incorrect-permission-assignment-for-critical-resource-vulnerability

Vendor	**MongoDB**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-92756, CVE-2026-92758, CVE-2026-92757, CVE-2026-93394, CVE-2026-93395, CVE-2026-93758, CVE-2026-93765, CVE-2026-93764, CVE-2026-93763, CVE-2026-93761, CVE-2026-93760, CVE-2026-93759)
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	MongoDB Entity Framework Core Provider: • 8.0.0 affects versions prior to 8.4.4 • 9.0.0 affects versions prior to 9.1.4 • 10.0.0 affects versions prior to 10.0.3 C Driver: • 2.0.0 affects versions prior to 2.3.2 Mongoid: • 9.1.0 • 9.0.0 affects 9.0.11 and prior versions • 8.1.0 affects 8.1.12 and prior versions • 8.0.0 affects 8.0.12 and prior versions • 7.2.0 affects 7.2.6 and prior versions • 7.3.0 affects 7.3.5 and prior versions • 7.4.0 affects 7.4.3 and prior versions • 7.5.0 affects 7.5.4 and prior versions • 7.6.0 affects 7.6.1 and prior versions
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 (CVE-2026-70906, CVE-2026-61308, CVE-2026-70907, CVE-2026-60589, CVE-2026-16440)
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 Master Data Management 5.1.3 to 5.3.1 patch 11 IBM Knowledge Catalog Neo4j On Cloud Pak for Data 5.0.0 to 5.3.1 patch 11 WebSphere Service Registry and Repository and Studio versions 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7288416 https://www.ibm.com/support/pages/node/7288406

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 16.04, 18.04, 20.04, 22.04, 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8714-3 https://ubuntu.com/security/notices/USN-8730-3 https://ubuntu.com/security/notices/USN-8761-2 https://ubuntu.com/security/notices/USN-8725-2 https://ubuntu.com/security/notices/USN-8715-2

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.