Advisory Alert

Alert Number: AAA20260724 **Date:** July 24, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
MongoDB	**Critical**	Buffer Overflow Vulnerability
F5	**High**	SQL injection Vulnerability
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
MongoDB	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-27727, CVE-2026-29145, CVE-2026-4800)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-27727:** mchange-commons-java, a library that provides Java utilities, includes code that mirrors early implementations of JNDI functionality, including support for remote `factoryClassLocation` values, by which code can be downloaded and invoked within a running application. **CVE-2026-29145:** CLIENT_CERT authentication does not fail as expected for some scenarios when soft fail is disabled vulnerability in Apache Tomcat, Apache Tomcat Native. **CVE-2026-4800:** When an application passes untrusted input as options.imports key names, an attacker can inject default-parameter expressions that execute arbitrary code at template compilation time. Additionally, _.template uses assignInWith to merge imports, which enumerates inherited properties via for..in. If Object.prototype has been polluted by any other vector, the polluted keys are copied into the imports object and passed to Function(). IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar versions 7.5.0 - 7.5.0 UP15 IF04 NTA versions 1.0.0 - 1.4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7280950 https://www.ibm.com/support/pages/node/7280949

Vendor	**MongoDB**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-13072)
Description	MongoDB has released a security update addressing a vulnerability that exists in their products. **CVE-2026-13072:** When compute mode is enabled on a standalone mongod instance, insufficient validation of externally sourced BSON data during aggregation pipeline processing can result in memory corruption, potentially leading to process termination or other unintended behavior. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MongoDB Server Versions: • 7.0 affects versions prior to 7.0.39 • 8.0 affects versions prior to 8.0.28 • 8.2.0 affects versions prior to 8.2.12 • 8.3.0 affects versions prior to 8.3.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://jira.mongodb.org/browse/SERVER-128494

Vendor	**F5**
Severity	**High**
Affected Vulnerability	SQL injection Vulnerability (CVE-2026-6476)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2026-6476:** SQL injection in PostgreSQL pg_createsubscriber allows an attacker with pg_create_subscription rights to execute arbitrary SQL as a superuser. The attack takes effect when pg_createsubscriber next runs. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next for Kubernetes versions: • 2.3.2 • 2.3.0 • 2.2.3 • 2.0.0 - 2.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000162387

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46323, CVE-2026-31684, CVE-2026-43190, CVE-2026-46152, CVE-2026-43279, CVE-2024-46738, CVE-2024-50076, CVE-2025-39982, CVE-2026-31488, CVE-2026-31613, CVE-2026-46116, CVE-2026-46209)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:44270 https://access.redhat.com/errata/RHSA-2026:44694 https://access.redhat.com/errata/RHSA-2026:44522 https://access.redhat.com/errata/RHSA-2026:44385

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	NTA versions 1.0.0 - 1.4.3 QRadar AI Assistant versions 1.0.0 - 2.0.0 InfoSphere Information Server versions 11.7.0.0 to 11.7.1.6 QRadar versions 7.5.0 - 7.5.0 UP15 IF04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7280949 https://www.ibm.com/support/pages/node/7280916 https://www.ibm.com/support/pages/node/7275287 https://www.ibm.com/support/pages/node/7280950

Vendor	**MongoDB**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-13078, CVE-2026-13077, CVE-2026-13076, CVE-2026-13075, CVE-2026-13074, CVE-2026-13073, CVE-2026-13071, CVE-2026-13070, CVE-2026-13069, CVE-2026-13068, CVE-2026-13067, CVE-2026-13066, CVE-2026-13065, CVE-2026-13064, CVE-2026-13063, CVE-2026-13062, CVE-2026-13061, CVE-2026-13060, CVE-2026-9737, CVE-2026-13059, CVE-2026-13058, CVE-2026-13057, CVE-2026-13056, CVE-2026-13055, CVE-2026-14881)
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 Server Versions: • 7.0 affects versions prior to 7.0.39 • 8.0 affects versions prior to 8.0.28 • 8.2.0 affects versions prior to 8.2.12 • 8.3.0 affects versions prior to 8.3.7 MongoDB Compass Versions: • 1.38.0 affects versions prior to 1.49.7
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.