Advisory Alert

Alert Number: AAA20261021 **Date:** October 21, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Oracle	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
MongoDB	**High**	Denial of Service Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
Zyxel Networks	**Medium**	Privilege Escalation Vulnerability

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-75595, CVE-2026-47691, CVE-2026-45674)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-75595:** io.netty.handler.ssl.SslClientHelloHandler#decode checks the wrong offset before reading the four-byte TLS handshake header, so a ClientHello whose handshake header spans records can cause an IndexOutOfBoundsException and invoke select(ctx, null). This selects the default SslContext instead of the SNI-specific context. In deployments where per-SNI clientAuth=REQUIRE is the sole mutual TLS gate, the default SslContext uses clientAuth=NONE or clientAuth=OPTIONAL, and no application-layer certificate verification exists, an unauthenticated remote attacker can bypass the protected route's mutual TLS requirement. **CVE-2026-47691:** Prior to versions 4.1.135.Final and 4.2.15.Final, Netty's `DnsResolveContext` insufficiently validates the bailiwick of NS records, enabling DNS Cache Poisoning. An attacker controlling an authoritative name server for a subdomain can poison the cache for parent domains (like `.co.uk`). **CVE-2026-45674:** Prior to versions 4.1.135.Final and 4.2.15.Final, Netty's DnsResolveContext fails to validate the origin (bailiwick) of CNAME records in DNS responses. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Guardium Data Protection versions 12.2.3, 12.1 and 12.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7293137 https://www.ibm.com/support/pages/node/7293136

Vendor	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle 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. Oracle 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://www.oracle.com/security-alerts/cpuoct2026.html https://www.oracle.com/security-alerts/bulletinoct2026.html

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-52935, CVE-2026-53196, CVE-2026-74588, CVE-2026-74752, CVE-2026-89479, CVE-2026-89631, CVE-2026-93288, CVE-2026-93817, CVE-2026-98320, CVE-2026-99999, CVE-2026-102994, CVE-2026-102998)
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 Platform & Enterprise Software: • Red Hat Quay Red Hat Enterprise Linux 8: • 8.10: Extended Life Cycle (x86_64) • Real Time & Real Time for NFV: x86_64 Red Hat Enterprise Linux 9: • 9.4: Advanced Update Support (AUS) (x86_64), Extended Life Cycle (all archs), 4 Years of Updates (aarch64, s390x), Update Services for SAP Solutions (ppc64le, x86_64) Red Hat Enterprise Linux 10: • Base RHEL 10 (aarch64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:86089 https://access.redhat.com/errata/RHSA-2026:85980 https://access.redhat.com/errata/RHSA-2026:85928 https://access.redhat.com/errata/RHSA-2026:85774

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53131, CVE-2026-63794, CVE-2026-63887, CVE-2026-68158)
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 Infrastructure: • openSUSE Leap 15.5 • SUSE Linux Enterprise 12 SP5: High Performance Computing, Live Patching, Server, Server for SAP Applications • SUSE Linux Enterprise 15 SP5: High Performance Computing, Live Patching, Real Time, Server, Server for SAP Applications • SUSE Linux Enterprise Micro 5.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264768-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264749-1/

Vendor	**MongoDB**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2026-112368)
Description	MongoDB has released a security update addressing a vulnerability that exists in their products. **CVE-2026-112368:** An uncontrolled recursion weakness in the BSON decoding logic of the MongoDB PHP driver may allow an unauthenticated party who can supply crafted binary document data to the decoder to exhaust the process stack. This may cause the PHP process using the driver to terminate unexpectedly, resulting in a loss of availability for that process. The condition occurs below the PHP layer and cannot be intercepted by application-level error handling. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PHP Driver versions: • affects versions prior to 1.21.12 • 2.1.0 affects versions prior to 2.1.12 • 2.5.0 affects versions prior to 2.5.5
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-2026-45673, CVE-2026-48043, CVE-2026-47244, CVE-2026-50560, CVE-2026-5704, CVE-2026-18508, CVE-2026-18477, CVE-2026-75596, CVE-2026-62243)
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 Guardium Data Protection versions 12.2.3, 12.1 and 12.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7293137 https://www.ibm.com/support/pages/node/7293136

Vendor	**Zyxel Networks**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-12489)
Description	Zyxel Networks has released a security update addressing a vulnerability that exists in their products. **CVE-2026-12489:** The incorrect authorization vulnerability in the DAL of certain firmware versions for 5G NR CPE, DSL/Ethernet CPE, Fiber ONTs, and Wireless Extenders could allow an authenticated attacker to elevate privileges by modifying the login_privilege data on an affected device. Zyxel Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Zyxel Infrastructure (Please refer to the link for model and version details): • 5G NR CPE • DSL/Ethernet CPE • Fiber ONTs • Wireless Extenders
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-incorrect-authorization-vulnerability-in-the-dal-of-certain-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-and-wireless-extenders-10-20-2026

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.