Advisory Alert

Alert Number: AAA20261016 **Date:** October 16, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-84961, CVE-2026-27727)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-84961:** undici's BalancedPool constructor passes its entire options object through an internal deep-clone that serializes and reparses the value as JSON. Because JSON cannot represent functions, any function-valued TLS option, such as a caller-supplied checkServerIdentity callback or a custom connector inside the connect option, is silently discarded before it reaches the TLS layer. As a result a peer whose certificate the application's custom checkServerIdentity was written to reject, but which still passes Node's default hostname and chain checks, is accepted when reached through BalancedPool. The Client, Pool, and Agent dispatchers are not affected because they extract the connect and tls options before cloning. **CVE-2026-27727:** mchange-commons-java includes its own JNDI-style dereferencing code, including support for remote factoryClassLocation values that let code be downloaded and run inside an application. If an attacker can get an application to read a crafted javax.naming.Reference or serialized object, they can trigger download and execution of malicious code. The JDK disabled this behavior by default via com.sun.jndi.ldap.object.trustURLCodebase, but libraries like c3p0 that resolve references through mchange-commons-java remained exposed. Version 0.4.0 fixes this by gating the functionality behind restrictive default settings, mirroring the JDK patch IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Disconnected Log Collector - Versions 1.0.0 - 2.0.0 • IBM Db2 Developer Extension - Versions 1.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7292743 • https://www.ibm.com/support/pages/node/7292731

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-74469, CVE-2026-80844, CVE-2026-81000, CVE-2026-2340, CVE-2026-3012, CVE-2026-5260, CVE-2026-54369, CVE-2026-58014, CVE-2026-58015, CVE-2026-42504)
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 OpenShift Container Platform 4.18, 4.17, 4.16, 4.13 & 4.12: • 4.18 for RHEL 9 & 8 (aarch64, ppc64le, s390x, x86_64) • 4.17 for RHEL 9 & 8 (aarch64, ppc64le, s390x, x86_64) • 4.16 for RHEL 9 (aarch64, ppc64le, s390x, x86_64) • 4.13 for RHEL 9 & 8 (aarch64, ppc64le, s390x, x86_64) • 4.12 for RHEL 9 & 8 (aarch64, ppc64le, s390x, x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:77612 • https://access.redhat.com/errata/RHSA-2026:77548 • https://access.redhat.com/errata/RHSA-2026:77320 • https://access.redhat.com/errata/RHSA-2026:77315 • https://access.redhat.com/errata/RHSA-2026:79035 • https://access.redhat.com/errata/RHSA-2026:77319

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53221, CVE-2026-53131, CVE-2025-38724, CVE-2025-21664, CVE-2024-57929, CVE-2024-57904, CVE-2024-57849, CVE-2024-56779, CVE-2024-56570, CVE-2024-53214, CVE-2024-53194)
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu - 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8922-2

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-18149, CVE-2026-18540, CVE-2026-19534, CVE-2026-84890, CVE-2026-84933, CVE-2026-84947, CVE-2026-85008, CVE-2026-85014, CVE-2026-85024, CVE-2026-64847, CVE-2026-59881, CVE-2026-69243, CVE-2026-69244, CVE-2026-54285, CVE-2026-69247, CVE-2026-69248, CVE-2026-69249, CVE-2026-75838, CVE-2026-104851, CVE-2026-87776, CVE-2026-101898, CVE-2026-101900, CVE-2026-101901, CVE-2026-101902, CVE-2026-101903, CVE-2026-101904, CVE-2026-101905, CVE-2026-101906, CVE-2026-101907, CVE-2026-101908, CVE-2026-101909, CVE-2026-75899, CVE-2026-75931, CVE-2026-75975, CVE-2026-76172, CVE-2026-68497, CVE-2026-83557, CVE-2026-19032, CVE-2026-91776, CVE-2026-91777, CVE-2026-18401, CVE-2026-84375, CVE-2026-84292, CVE-2026-84394, CVE-2026-101294, CVE-2026-105442)
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	• WebSphere Application Server Versions 8.5 - 9.0 • WebSphere Application Server - Liberty 17.0.0.3 - 26.0.0.10 • IBM Security Verify Governance Adapter for CyberArk - Versions 10.0.1 • Disconnected Log Collector - Versions 1.0.0 - 2.0.0 • IBM Db2 Developer Extension - Versions 1.2.0 • watsonx Code Assistant On Prem - Versions 5.1.0 to 5.3.1 Patch 14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7292221 • https://www.ibm.com/support/pages/node/7292235 • https://www.ibm.com/support/pages/node/7292634 • https://www.ibm.com/support/pages/node/7292742 • https://www.ibm.com/support/pages/node/7292737 • https://www.ibm.com/support/pages/node/7292647 • https://www.ibm.com/support/pages/node/7292743 • https://www.ibm.com/support/pages/node/7292731

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.