



Advisory Alert

Alert Number: AAA20260112

Date: January 12, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	High , Medium	Multiple Vulnerabilities
IBM	Medium	Multiple Vulnerabilities

Description

Affected Product	Red Hat
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39806, CVE-2025-39840, CVE-2025-39883, CVE-2025-40240, CVE-2025-39993, CVE-2025-68285)
Description	<p>Red Hat has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems.</p> <p>Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.</p>
Affected Products	<p>Red Hat CodeReady Linux Builder for ARM 64 8 aarch64</p> <p>Red Hat CodeReady Linux Builder for ARM 64 9 aarch64</p> <p>Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x</p> <p>Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le</p> <p>Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le</p> <p>Red Hat CodeReady Linux Builder for x86_64 8 x86_64</p> <p>Red Hat CodeReady Linux Builder for x86_64 9 x86_64</p> <p>Red Hat Enterprise Linux for ARM 64 8 aarch64</p> <p>Red Hat Enterprise Linux for ARM 64 9 aarch64</p> <p>Red Hat Enterprise Linux for IBM z Systems 8 s390x</p> <p>Red Hat Enterprise Linux for IBM z Systems 9 s390x</p> <p>Red Hat Enterprise Linux for Power, little endian 8 ppc64le</p> <p>Red Hat Enterprise Linux for Power, little endian 9 ppc64le</p> <p>Red Hat Enterprise Linux for Real Time 8 x86_64</p> <p>Red Hat Enterprise Linux for Real Time for NFV 8 x86_64</p> <p>Red Hat Enterprise Linux for x86_64 8 x86_64</p> <p>Red Hat Enterprise Linux for x86_64 9 x86_64</p>
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none"> https://access.redhat.com/errata/RHSA-2026:0445 https://access.redhat.com/errata/RHSA-2026:0443 https://access.redhat.com/errata/RHSA-2026:0444

Affected Product	IBM
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-53057, CVE-2025-30754)
Description	<p>IBM has released a security update addressing multiple vulnerabilities that exists in their products.</p> <p>CVE-2025-53057: An unspecified vulnerability in Java SE related to the Security component could allow a remote attacker to cause no confidentiality impact, high integrity impact, and no availability impact.</p> <p>CVE-2025-30754: A vulnerability exists in the Java Secure Socket Extension (JSSE) component of Oracle Java SE and Oracle GraalVM that can be exploited by an unauthenticated remote attacker over a TLS network connection. Although exploitation is difficult, a successful attack could compromise the Java security model, allowing unauthorized reading, modification, insertion, or deletion of accessible application data.</p> <p>IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.</p>
Affected Products	<p>DB2 10.5.0 - 10.5.11 Client and Server</p> <p>DB2 11.1.4.0 - 11.1.4.7 Client and Server</p> <p>DB2 11.5.4.0 - 11.5.9.0 Client and Server</p> <p>DB2 12.1.0 - 12.1.3 Client and Server</p>
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7256635

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.