Advisory Alert

Alert Number: AAA20261110 **Date:** November 10, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-90711, CVE-2026-41586)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-90711:** proxy-addr is a Node.js module that determines a request's client address behind trusted reverse proxies, and it backs Express req.ip and req.ips. In versions 1.1.0 through 2.0.7, a trust subnet written in IPv4-mapped IPv6 notation with an IPv4-sized prefix, such as ::ffff:10.0.0.0/8 instead of the correct ::ffff:10.0.0.0/104, is accepted without error but trusts every IPv4 address on the internet rather than the block it names. Because the socket peer then becomes trusted at hop 0, any unauthenticated client can supply an arbitrary X-Forwarded-For header and control the address the application reads, which defeats IP-based access control, rate limiting, geolocation, and audit logging. **CVE-2026-41586:** Hyperledger Fabric is an enterprise-grade permissioned distributed ledger framework for developing solutions and applications. From versions 1.0.0 to 2.2.26, Channel.java implements readObject() and exposes deSerializeChannel() which call ObjectInputStream.readObject() on untrusted byte arrays without configuring an ObjectInputFilter. This is a classic Java deserialization RCE pattern. At time of publication, there are no publicly available patches. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Big SQL on Cloud Pak for Data - IBM Big SQL on Cloud Pak for Data 5.0 IBM Big SQL on Software Hub - IBM Big SQL on Cloud Pak for Data 5.1 IBM Big SQL on Software Hub - IBM Big SQL on Software Hub 5.2 IBM Big SQL on Software Hub - IBM Big SQL on Software Hub 5.3 IBM Big SQL on Software Hub - IBM Big SQL on Software Hub 5.4 up to patch 7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7295981

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-98432, CVE-2026-12080, CVE-2026-14456, CVE-2026-26007, CVE-2026-68376, CVE-2026-77214, CVE-2026-80824, CVE-2026-89777, CVE-2026-94453, CVE-2026-98222, CVE-2025-31936, CVE-2026-18798, CVE-2026-63072, CVE-2026-63076, CVE-2026-71226, CVE-2026-77206, CVE-2026-77207, CVE-2026-90003, CVE-2026-98320, CVE-2026-16313, CVE-2026-45447, CVE-2026-59999, CVE-2026-60002, CVE-2026-80792, CVE-2026-89846, CVE-2026-111497, CVE-2025-47273, CVE-2026-28390, CVE-2026-34182, CVE-2026-42011, CVE-2026-42013, CVE-2026-45445, CVE-2026-59995)
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 4.12 for RHEL 9 x86_64 Red Hat OpenShift Container Platform 4.12 for RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 4.12 for RHEL 9 ppc64le Red Hat OpenShift Container Platform for Power 4.12 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.12 for RHEL 9 s390x Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.12 for RHEL 8 s390x Red Hat OpenShift Container Platform for ARM 64 4.12 for RHEL 9 aarch64 Red Hat OpenShift Container Platform for ARM 64 4.12 for RHEL 8 aarch64 Red Hat OpenShift Container Platform 5.0 for RHEL 10 x86_64 Red Hat OpenShift Container Platform 5.0 for RHEL 9 x86_64 Red Hat OpenShift Container Platform 5.0 for RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 5.0 for RHEL 10 ppc64le Red Hat OpenShift Container Platform for Power 5.0 for RHEL 9 ppc64le Red Hat OpenShift Container Platform for Power 5.0 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 5.0 for RHEL 10 s390x Red Hat OpenShift Container Platform for IBM Z and LinuxONE 5.0 for RHEL 9 s390x Red Hat OpenShift Container Platform for IBM Z and LinuxONE 5.0 for RHEL 8 s390x Red Hat OpenShift Container Platform for ARM 64 5.0 for RHEL 10 aarch64 Red Hat OpenShift Container Platform for ARM 64 5.0 for RHEL 9 aarch64 Red Hat OpenShift Container Platform for ARM 64 5.0 for RHEL 8 aarch64 Red Hat OpenShift Container Platform 4.14 for RHEL 9 x86_64 Red Hat OpenShift Container Platform 4.14 for RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 4.14 for RHEL 9 ppc64le Red Hat OpenShift Container Platform for Power 4.14 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 9 s390x Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 8 s390x Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 9 aarch64 Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 8 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:95416 • https://access.redhat.com/errata/RHSA-2026:94537 • https://access.redhat.com/errata/RHSA-2026:95508

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76166, CVE-2026-86247, CVE-2026-78383, CVE-2026-77791, CVE-2026-86350, CVE-2026-76183, CVE-2026-79677, CVE-2026-73581, CVE-2026-86248, CVE-2026-86243, CVE-2026-86246, CVE-2026-39821, CVE-2026-92092)
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	JBoss Enterprise Web Server 6 for RHEL 10 x86_64 JBoss Enterprise Web Server 6 for RHEL 9 x86_64 JBoss Enterprise Web Server 6 for RHEL 8 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 Red Hat OpenShift Container Platform 4.14 for RHEL 9 x86_64 Red Hat OpenShift Container Platform 4.14 for RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 4.14 for RHEL 9 ppc64le Red Hat OpenShift Container Platform for Power 4.14 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 9 s390x Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 8 s390x Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 9 aarch64 Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 8 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:96228 • https://access.redhat.com/errata/RHSA-2026:96229 • https://access.redhat.com/errata/RHSA-2026:95507

Vendor	**Asus**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-88710, CVE-2026-88709, CVE-2026-88708, CVE-2026-88707)
Description	Asus 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. Asus advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ASUS Router Firmware: • 3.0.0.4_386 series • 3.0.0.4_388 series • 3.0.0.6_102 series
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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 Big SQL on Cloud Pak for Data - IBM Big SQL on Cloud Pak for Data 5.0 IBM Big SQL on Software Hub - IBM Big SQL on Cloud Pak for Data 5.1 IBM Big SQL on Software Hub - IBM Big SQL on Software Hub 5.2 IBM Big SQL on Software Hub - IBM Big SQL on Software Hub 5.3 IBM Big SQL on Software Hub - IBM Big SQL on Software Hub 5.4 up to patch 7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7295981

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.