Advisory Alert

Alert Number: AAA20260209 **Date:** February 9, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**Critical**	Authentication Bypass Vulnerability
Fortinet	**Critical**	SQL Injection Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-1709)
Description	Red Hat has released a security update addressing a vulnerability that exists in the Keylime component in their Products. **CVE-2026-1709 -** This authentication bypass vulnerability allows unauthenticated clients with network access to perform administrative operations, including listing agents, retrieving public Trusted Platform Module (TPM) data, and deleting agents, by connecting without presenting a client certificate. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:2225

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2026-21643)
Description	Fortinet has released security updates addressing a vulnerability that exists in their FortiClientEMS products. **CVE-2026-21643**– An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in the FortiClientEMS 7.4.4 may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiClientEMS version 7.4.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-25-1142

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-47913, CVE-2025-47914, CVE-2025-58181, CVE-2026-1188)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale IBM Storage Scale versions 6.0.0.0 and 5.2.3.0 to 5.2.3.5 WebSphere Service Registry and Repository Studio 8.5 to 8.5.6.3 WebSphere Service Registry and Repository 8.5 to 8.5.6.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7260042 https://www.ibm.com/support/pages/node/7259945

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.