Advisory Alert

Alert Number: AAA20260227 **Date:** February 27, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Buffer Overflow Vulnerability
Juniper	**Critical**	Improper Access Control Vulnerability
IBM	**High**	Multiple Vulnerabilities
Broadcom VMware	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2025-68615)
Description	IBM has released a security update addressing a vulnerability that exists in their QRadar products. **CVE-2025-68615**: net-snmp is a SNMP application library, tools and daemon. Prior to versions 5.9.5 and 5.10.pre2, a specially crafted packet to a net-snmp snmptrapd daemon can cause a buffer overflow and the daemon to crash. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QRadar versions 7.5.0 to 7.5.0 UP14 IF04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7261935

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2026-21902)
Description	Juniper has released a security update addressing a vulnerability that exists in the Junos OS Evolved PTX Series. **CVE-2026-21902**: An Incorrect Permission Assignment for Critical Resource vulnerability in the On-Box Anomaly detection framework of Juniper Networks Junos OS Evolved on PTX Series allows an unauthenticated, network-based attacker to execute code as root. Juniper advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Junos OS Evolved on PTX Series 25.4 versions before 25.4R1-S1-EVO, 25.4R2-EVO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://supportportal.juniper.net/s/article/2026-02-Out-of-Cycle-Security-Bulletin-Junos-OS-Evolved-PTX-Series-A-vulnerability-allows-a-unauthenticated-network-based-attacker-to-execute-code-as-root-CVE-2026-21902

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-13601, CVE-2025-9230, CVE-2023-53673, CVE-2025-40154, CVE-2025-40248, CVE-2025-40277, CVE-2025-68973, CVE-2025-39993, CVE-2025-40240, CVE-2025-68285)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their QRadar 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	QRadar versions 7.5.0 to 7.5.0 UP14 IF04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7261935

Affected Product	**Broadcom VMware**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22715, CVE-2026-22716, CVE-2026-22717, CVE-2026-22722)
Description	Broadcom 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. Broadcom advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	VMware Workstation version 17.x, 25H2 VMware Fusion version 13.x, 25H2 (MacOS only)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/36986

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.