Advisory Alert

Alert Number: AAA20260817 **Date:** August 17, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-16885, CVE-2026-17118, CVE-2026-17152, CVE-2026-15065, CVE-2026-16926, CVE-2026-17141, CVE-2026-16656, CVE-2026-17422, CVE-2026-17142, CVE-2026-16862, CVE-2026-18835, CVE-2026-17122, CVE-2026-16872, CVE-2026-16816, CVE-2026-60002, CVE-2026-17160, CVE-2026-16839, CVE-2026-16439, CVE-2026-16903, CVE-2026-15068, CVE-2026-16894, CVE-2026-17157, CVE-2026-16822, CVE-2026-17136, CVE-2026-16864, CVE-2026-17145, CVE-2026-16840, CVE-2026-16919, CVE-2026-16913, CVE-2026-16834, CVE-2026-16882, CVE-2026-16845, CVE-2026-16917, CVE-2026-12087, CVE-2026-17040, CVE-2026-16835, CVE-2026-16687, CVE-2026-45623)
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	AIX versions 7.2 and 7.3 PowerVM VIOS versions 4.1 Power Systems Server Firmware versions: • FW1120.00 • FW1110.00 to FW1110.30 • FW1060.00 to FW1060.80 • FW950.00 to FW950.H2 Network Threat Analytics App versions 1.0.0 to 2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7283858 https://www.ibm.com/support/pages/node/7283894 https://www.ibm.com/support/pages/node/7283893 https://www.ibm.com/support/pages/node/7283821

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	AIX versions 7.2 and 7.3 PowerVM VIOS versions 4.1 Network Threat Analytics App versions 1.0.0 to 2.0.0 Power Systems Server Firmware versions: • FW1120.00 • FW1110.00 to FW1110.30 • FW1060.00 to FW1060.80 • FW950.00 to FW950.H2 PowerVM Hypervisor versions: • FW1120.00 • FW1110.00 to FW1110.20 • FW1060.00 to FW1060.71 • FW950.00 to FW950.H2 Power Systems Virtualization Management Interface versions: • FW1110.00 to FW1110.30 • FW1120.00 to FW1120.00 • FW1060.00 to FW1060.80 Power Systems Firmware: • FW1120.00 • FW1110.00 to FW1110.30 • FW1060.00 to FW1060.80 • FW950.00 to FW950.H2 • OP940.00 to OP940.a1 (Power9) • OP940.00 to OP940.81 (Power HMC) QRadar SIEM Network Threat Analytics App versions 1.0.0 to 2.0.0 QRadar Log Source Management App verions 1.0.0 to 7.0.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/

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.