Advisory Alert

Alert Number: AAA20260609 **Date:** June 9, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Broadcom	**High**	Cross-Site Scripting Vulnerabilities
Check Point	**High**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-8633, CVE-2026-8644, CVE-2026-9319, CVE-2026-9311)
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	IBM Cloud Pak for Applications Versions 5.1, 5.2 and 5.3 IBM WebSphere Hybrid Edition Version 5.1 IBM WebSphere Application Server Versions: • 8.5 and 9.0 • 9.0.0.0 to 9.0.5.27 • 8.5.5.0 to 8.5.5.29 IBM Web Server Plug-ins for IBM WebSphere Application Server Versions 8.5 and 9.0 IBM WebSphere Liberty Versions 8.5 and 9.0 IBM WebSphere Application Server Liberty Versions 17.0.0.3 to 26.0.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7275533 https://www.ibm.com/support/pages/node/7275420 https://www.ibm.com/support/pages/node/7275461 https://www.ibm.com/support/pages/node/7275462 https://www.ibm.com/support/pages/node/7275419 https://www.ibm.com/support/pages/node/7275528 https://www.ibm.com/support/pages/node/7274072 https://www.ibm.com/support/pages/node/7274738

Vendor	**Broadcom**
Severity	**High**
Affected Vulnerability	Cross-Site Scripting Vulnerabilities (CVE-2026-41722, CVE-2026-41723, CVE-2026-41724)
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 Aria Operations VMware Cloud Foundation Operations VMware Cloud Foundation VMware vSphere Foundation VMware Telco Cloud Platform
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37513

Vendor	**Check Point**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-50751, CVE-2026-50752)
Description	Check Point has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-50751**: An attacker can bypass user authentication by exploiting a logic flow weakness in the Remote Access and Mobile Access certificate validation and establish a remote access VPN connection without a valid user password. **CVE-2026-50752**: A vulnerability in the certificate validation logic of the deprecated IKEv1 key exchange method may lead to a man-in-the-middle attack on the VPN site-to-site configuration. Check Point advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	R82.10 Jumbo Hotfix Take 19 or below R82 Jumbo Hotfix Take 103 or below R81.20 Jumbo Hotfix Take 141 or below R81.10 (EOS) R81 (EOS) R80.40 (EOS) Spark Firewalls: R80.20.X (EOS), R81.10.X, R82.00.X
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk185033 https://support.checkpoint.com/results/sk/sk185035

Vendor	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11187, CVE-2025-15467, CVE-2025-15468, CVE-2025-15469, CVE-2025-66199, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2025-60876, CVE-2026-22795, CVE-2026-22796, CVE-2026-28262)
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerScale Node Firmware Package Versions prior to 13.2.5 on: • PowerScale B100 • PowerScale F200 • PowerScale F600 • PowerScale F900 • PowerScale P100 • PowerScale F210 • PowerScale F710 • PowerScale F910 • PowerScale PA110 iDRAC Tools Versions prior to 11.4.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000474822/dsa-2026-237-security-update-for-dell-powerscale-onefs-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000474864/dsa-2026-239-security-update-for-dell-idrac-tools-vulnerability

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-8620, CVE-2026-4410, CVE-2026-5516, CVE-2026-33532, CVE-2026-41238, CVE-2026-41239, CVE-2026-41240, CVE-2026-44431, CVE-2026-44432, CVE-2026-6321, CVE-2025-13465, CVE-2026-2950, CVE-2026-9330)
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	IBM Cloud Pak for Applications Versions 5.1, 5.2 and 5.3 Platform Navigator in IBM Cloud Pak for Integration (CP4I) Versions: • 16.1.0 to 16.1.0.24 • 16.1.1 • 16.1.2 • 16.1.3.0 to 16.1.3.5 Automation Assets in IBM Cloud Pak for Integration (CP4I) Versions: • 4.0.0-sc2 to 4.0.21-sc2 • 4.1.0 • 4.2.0 • 4.3.0 to 4.3.4 IBM WebSphere Hybrid Edition Version 5.1 IBM WebSphere Application Server Liberty Versions 17.0.0.3 to 26.0.0.5 IBM WebSphere Application Server Versions: • 9.0.0.0 to 9.0.5.28 • 8.5.5.0 to 8.5.5.29 IBM Enterprise Application Runtimes Versions 1.0 and 1.1
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.