Advisory Alert

Alert Number: AAA20260608 **Date:** June 8, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Cisco	**High**	Privilege Escalation Vulnerability
Dell	**High**	Local Privilege Escalation Vulnerability
NetApp	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-4800, CVE-2026-33186, CVE-2026-6951, CVE-2026-42043, CVE-2026-42044, CVE-2025-62718)
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 Storage Scale Versions: • 6.0.0.0 - 6.0.0.2 • 5.2.0.0 - 5.2.3.7 Automation Assets in IBM Cloud Pak for Integration (CP4I) Versions: • 4.0.0-sc2 to 4.0.20-sc2 • 4.1.0, 4.2.0, 4.3.0 • 4.3.1 to 4.3.4 Platform Navigator in IBM Cloud Pak for Integration (CP4I) • 16.1.1 to 16.1.2 • 16.1.3.0 to 16.1.3.5 • 16.1.0 to 16.1.0.23 IBM Big SQL on Cloud Pak for Data • IBM Db2 Big SQL 7.6 on Cloud Pak for Data 4.8 • IBM Db2 Big SQL 7.7 on Cloud Pak for Data 5.0 • IBM Db2 Big SQL 7.8 on Cloud Pak for Data 5.1 • IBM Db2 Big SQL 8.2 on Cloud Pak for Data 5.2 • IBM Db2 Big SQL 8.3.0, 8.3.1 on Cloud Pak for Data 5.3.0, 5.3.1 up to patch 3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7275270 • https://www.ibm.com/support/pages/node/7275242 • https://www.ibm.com/support/pages/node/7273112 • https://www.ibm.com/support/pages/node/7275256

Vendor	**Cisco**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-20245)
Description	Cisco has released security updates addressing a vulnerability that exists in their products. **CVE-2026-20245**: A vulnerability in the CLI of Cisco Catalyst SD-WAN Manager. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by uploading a crafted file to the affected system. A successful exploit could allow the attacker to perform command injection attacks on an affected system and elevate their privileges as the root user. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Cisco Catalyst SD-WAN Manager
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Local Privilege Escalation Vulnerability (CVE-2026-31431)
Description	Dell has released security updates addressing a vulnerability that exists in the third party components of their products. **CVE-2026-31431**: In the Linux kernel, the following vulnerability has been resolved: crypto: algif_aead - Revert to operating out-of-place This mostly reverts commit 72548b093ee3 except for the copying of the associated data. There is no benefit in operating in-place in algif_aead since the source and destination come from different mappings. Get rid of all the complexity added for in-place operation and just copy the AD directly. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Dell Automation Platform - Versions prior to 2.1.0.0 • Dell VxRail Appliance - Versions prior to 8.0.390
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000473635/dsa-2026-245-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000473583/dsa-2026-244-security-update-for-dell-automation-platform-for-multiple-third-party-component-vulnerabilities

Vendor	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-7345, CVE-2025-14512, CVE-2025-14087)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-7345**: Multiple NetApp products incorporate GDK-Pixbuf. GDK-Pixbuf versions through 2.43.3 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2025-14512**: Multiple NetApp products incorporate GLib. GLib versions prior to 2.86.3 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2025-14087**: Multiple NetApp products incorporate GLib. GLib versions prior to 2.86.3 and 2.87.0 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20260605-0002 • https://security.netapp.com/advisory/ntap-20260605-0003 • https://security.netapp.com/advisory/ntap-20260605-0006

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-2950, CVE-2026-24281, CVE-2026-24308, CVE-2026-42033, CVE-2026-42034, CVE-2026-42035, CVE-2026-42036, CVE-2026-42037, CVE-2026-42038, CVE-2026-42039, CVE-2026-42040, CVE-2026-42041, CVE-2026-42042, CVE-2026-26996, CVE-2026-27903, CVE-2026-27904, CVE-2026-2739, CVE-2026-24051, CVE-2025-33042, CVE-2026-9167)
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 Storage Scale Versions: • 6.0.0.0 - 6.0.0.2 • 5.2.0.0 - 5.2.3.7 Automation Assets in IBM Cloud Pak for Integration (CP4I) Versions: • 4.0.0-sc2 to 4.0.20-sc2 • 4.1.0, 4.2.0, 4.3.0 • 4.3.1 to 4.3.4 Platform Navigator in IBM Cloud Pak for Integration (CP4I) • 16.1.1 to 16.1.2 • 16.1.3.0 to 16.1.3.5 • 16.1.0 to 16.1.0.23 IBM Big SQL on Cloud Pak for Data • IBM Db2 Big SQL 7.6 on Cloud Pak for Data 4.8 • IBM Db2 Big SQL 7.7 on Cloud Pak for Data 5.0 • IBM Db2 Big SQL 7.8 on Cloud Pak for Data 5.1 • IBM Db2 Big SQL 8.2 on Cloud Pak for Data 5.2 • IBM Db2 Big SQL 8.3.0, 8.3.1 on Cloud Pak for Data 5.3.0, 5.3.1 up to patch 3 IBM Storage Scale Container Native and CSI • Storage Scale Container Native 6.0.0.0 - 6.0.0.2 / CSI 3.0.0 - 3.0.2 • Storage Scale Container Native 5.2.3.0 - 5.2.3.7 / CSI 2.14.0 - 2.14.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7275270 • https://www.ibm.com/support/pages/node/7273112 • https://www.ibm.com/support/pages/node/7275257 • https://www.ibm.com/support/pages/node/7275269 • https://www.ibm.com/support/pages/node/7275286

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.