Advisory Alert

Alert Number: AAA20260430 **Date:** April 30, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
SonicWall	**High**	Multiple Vulnerabilities
MongoDB	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities
Dell	**Medium**	Type Confusion Vulnerability
HP	**Medium**	Improper Input Validation Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exists in the third-party components of their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell SmartFabric Manager – Versions prior to 2.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000458847/dsa-2026-207-security-update-for-dell-smartfabric-manager-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-29000, CVE-2026-29063, CVE-2026-33202, CVE-2026-32871, CVE-2026-33195, CVE-2026-1615, CVE-2025-69872, CVE-2026-33937)
Description	IBM has released a security update addressing multiple vulnerabilities that exists in their product. 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 Cloud Pak for AIOps – Versions 4.1.0 - 4.13.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7271152

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0204, CVE-2026-0205, CVE-2026-0206)
Description	SonicWall has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-0204:** A vulnerability in the access control mechanism of SonicOS may allow certain management interface functions to be accessible under specific conditions. **CVE-2026-0205:** A post-authentication Path Traversal vulnerability in SonicOS allows an attacker to interact with usually restricted services. **CVE-2026-0206:** A post-authentication Stack-based Buffer Overflow vulnerabilities in SonicOS allows a remote attacker to crash a firewall. SonicWall advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	6.5.5.1-6n and older versions • Gen6 Hardware Firewalls - SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2650, NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350WSM Series - SM 9200, SM 9250, SM 9400, SM 9450, SM 9600, SM 9650 Versions 7.0.1-5169 & 7.3.1-7013 and older • Gen7 NSv - NSv 270, NSv 470, NSv 870 • Gen7 Firewalls - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700, Gen7 NSv - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure) 8.1.0-8017 and older versions • Gen8 Firewalls - TZ80, TZ280, TZ380, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0004

Affected Product	**MongoDB**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6914, CVE-2026-6915)
Description	MongoDB has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2026-6914:** Computing the MD5 checksum of a malformed BSON object under specific conditions may cause loss of availability in MongoDB server. This issue affects all MongoDB Server v8.2 versions, all MongoDB Server v8.1 versions, MongoDB Server v8.0 versions prior to 8.0.21, MongoDB Server v7.0 versions prior to 7.0.32 **CVE-2026-6915:** An authorization flaw in the user management command could allow an authenticated user to make limited changes to authentication-related data associated with another user account. This could affect how authentication is performed for the impacted account. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MongoDB Server • 8.2.0 affects versions prior to 8.2.7 • 8.1.0 affects 8.1.* and prior versions • 8.0.0 affects versions prior to 8.0.21 • 7.0.0 affects versions prior to 7.0.32
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://jira.mongodb.org/browse/SERVER-119679 https://jira.mongodb.org/browse/SERVER-119981

Affected Product	**IBM**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22737, CVE-2025-13465, CVE-2026-22735, CVE-2026-33916, CVE-2026-3497, CVE-2026-33036, CVE-2025-15467, CVE-2023-40403, CVE-2024-35255, CVE-2024-47764, CVE-2025-30153, CVE-2026-26961, CVE-2026-33169, CVE-2026-33170, CVE-2026-33173, CVE-2026-33174, CVE-2026-33176, CVE-2026-33306, CVE-2026-34230, CVE-2026-34444, CVE-2026-34763, CVE-2026-34785, CVE-2026-34786, CVE-2026-34826, CVE-2026-34829, CVE-2026-34830, CVE-2026-34831, CVE-2026-35611, CVE-2026-4147, CVE-2026-4148, CVE-2026-4358, CVE-2026-5170, CVE-2025-6176, CVE-2025-69419, CVE-2025-13466, CVE-2025-66199, CVE-2025-66030, CVE-2025-66031, CVE-2025-9086, CVE-2026-39407, CVE-2026-39408, CVE-2026-39409, CVE-2026-39410, CVE-2026-33938, CVE-2026-33939, CVE-2026-33940, CVE-2026-33941, CVE-2026-34601, CVE-2026-27124, CVE-2025-5115, CVE-2026-31988, CVE-2026-39406, CVE-2025-14104, CVE-2026-30922, CVE-2026-34070, CVE-2026-33349, CVE-2025-12816, CVE-2025-10158, CVE-2026-28277, CVE-2026-0861, CVE-2026-1642, CVE-2025-64340, CVE-2025-69196, CVE-2025-69720, CVE-2025-66566, CVE-2026-3520, CVE-2026-40087, CVE-2025-11187)
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 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 - 7.5.0 UP15 IF01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7270594

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Type Confusion Vulnerability (CVE-2026-22796)
Description	Dell has released a security update addressing a vulnerability that exists in their products. **CVE-2026-22796:** A type confusion vulnerability exists in the signature verification of signed PKCS#7 data where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid or NULL pointer dereference when processing malformed PKCS#7 data. Impact summary: An application performing signature verification of PKCS#7 data or calling directly the PKCS7_digest_from_attributes() function can be caused to dereference an invalid or NULL pointer when reading, resulting in a Denial of Service. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000458870/dsa-2026-136-security-update-for-dell-poweredge-server-for-an-openssl-vulnerability

Affected Product	**HP**
Severity	**Medium**
Affected Vulnerability	Improper Input Validation Vulnerability (CVE-2025-33043)
Description	HP has released a security update addressing a vulnerability that exists in their products. **CVE-2025-33043:** APTIOV contains a vulnerability in BIOS where an attacker may cause an Improper Input Validation locally. Successful exploitation of this vulnerability can potentially impact of integrity. HP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hp.com/us-en/document/ish_14838322-14839257-16/hpsbhf04112

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.