Advisory Alert

Alert Number: AAA20260514 **Date:** May 14, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
cPanel	**Critical**	Heap buffer overflow Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
F5	**Critical**	Incorrect Use of Privileged APIs Vulnerability
MongoDB	**Critical**	Command Injection Vulnerability
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**, Medium	Multiple Vulnerabilities
F5	**High**, Medium	Multiple Vulnerabilities
Palo Alto Networks	**High**, Medium	Multiple Vulnerabilities
MongoDB	**High**, Medium, Low	Multiple Vulnerabilities
Drupal	**High**, Medium, Low	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
HP	Medium	Privilege Escalation Vulnerability
cPanel	Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**cPanel**
Severity	**Critical**
Affected Vulnerability	Heap buffer overflow Vulnerability (CVE-2026-42945)
Description	cPanel has released a security update addressing a vulnerability that exist in their products. **CVE-2026-42945** - This vulnerability exists in the ngx_http_rewrite_module module of NGINX Plus and NGINX Open Source products. An unauthenticated attacker along with conditions beyond its control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, for systems with Address Space Layout Randomization (ASLR) disabled, code execution is possible. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 • ea-nginx version v1.30.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/#2560

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-62718, CVE-2025-6547, CVE-2025-6545, CVE-2025-43859)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their products. 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	Platform Navigator in IBM Cloud Pak for Integration (CP4I) versions: • 16.1.0 to 16.1.0.22 • 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 4.0.19-sc2 • 4.1.0 • 4.2.0 • 4.3.0 to 4.3.3 IBM Watson Knowledge Catalog on-prem versions: • 5.0.0, 5.0.1, 5.0.2, 5.0.3, 5.1.0, 5.1.1, 5.1.2, 5.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7272806 https://www.ibm.com/support/pages/node/7272836

Affected Product	**F5**
Severity	**Critical**
Affected Vulnerability	Incorrect Use of Privileged APIs Vulnerability (CVE-2026-41225)
Description	F5 has released a security update addressing a vulnerability that exists in their product. **CVE-2026-41225:** A vulnerability exists in iControl REST where a highly privileged, authenticated attacker with at least the Manager role can create configuration objects that allow running arbitrary commands. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) • 21.0.0 • 17.5.0 - 17.5.1 • 17.1.0 - 17.1.3 • 16.1.0 - 16.1.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000160916

Affected Product	**MongoDB**
Severity	**Critical**
Affected Vulnerability	Command Injection Vulnerability (CVE-2026-8431)
Description	MongoDB has released a security update addressing a vulnerability that exists in their product. **CVE-2026-8431:** An administrative user with access to configure webhooks can execute arbitrary commands by configuring and then triggering webhooks containing specific FreeMarker template syntax. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ops Manager 7.0 affects versions prior to 8.0.23
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/docs/ops-manager/current/release-notes/application/#onprem-server-8.0.23

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54518, CVE-2025-69421, CVE-2025-69420, CVE-2025-69419, CVE-2026-22795, CVE-2026-22796, CVE-2025-68160, CVE-2025-69418)
Description	Dell 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. Dell advises to apply security fixes at your earliest to protect 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/000440810/dsa-2026-144 https://www.dell.com/support/kbdoc/en-us/000420412/dsa-2026-069

Affected Product	**SUSE**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43284, CVE-2026-43500)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-43284:** The Linux kernel has been updated to prevent in-place decryption on shared socket buffer (skb) fragments in the XFRM ESP subsystem. Previously, the IPv4/IPv6 datagram paths failed to set the SKBFL_SHARED_FRAG flag when using MSG_SPLICE_PAGES, causing ESP to incorrectly decrypt data in place on memory still shared with external pipes. The fix ensures these fragments are correctly flagged, forcing ESP input to utilize skb_cow_data() to create private copies before decryption. This change secures externally backed fragments while maintaining the existing fast path for private nonlinear fragments and leaving ESP output logic unchanged, as it already handles nonlinear buffers safely. **CVE-2026-43500:** The Linux kernel has been updated to prevent in-place decryption on shared data and response packets within the rxrpc protocol. Previously, packets were only unshared if the socket buffer was cloned, allowing externally-owned paged fragments—such as those created via splice()—to bypass security safeguards and undergo in-place decryption. The fix extends the unsharing requirement to include any buffer with a fragment list or shared fragments, effectively closing the splice-loopback vulnerability. This adjustment ensures that externally-shared fragments are safely copied to linear buffers before processing while preserving the zero-copy fast path for private kernel fragments. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP6 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP6 Basesystem Module 15-SP7 Development Tools Module 15-SP7 Legacy Module 15-SP7 Public Cloud Module 15-SP7 SUSE Linux Enterprise Desktop 15 SP7 SUSE Linux Enterprise High Availability Extension 15 SP7 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Linux Enterprise Workstation Extension 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20261840-2/ https://www.suse.com/support/update/announcement/2026/suse-su-20261840-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261825-1/

Affected Product	**F5**
Severity	**High,** **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-41953, CVE-2026-42063, CVE-2026-32643, CVE-2026-40631, CVE-2026-39455, CVE-2026-42406, CVE-2026-41217, CVE-2026-34176, CVE-2026-32673, CVE-2026-41959, CVE-2026-42937, CVE-2026-39459, CVE-2026-42058, CVE-2026-39458, CVE-2026-24464, CVE-2026-42930, CVE-2026-42926, CVE-2026-40699, CVE-2026-35062, CVE-2026-40629, CVE-2026-42781, CVE-2026-41954, CVE-2026-42780, CVE-2026-41219, CVE-2026-40618, CVE-2026-42934, CVE-2026-42946, CVE-2026-40462, CVE-2026-42409, CVE-2026-34019, CVE-2026-40460, CVE-2026-40061, CVE-2026-41956, CVE-2026-42924, CVE-2026-42919, CVE-2026-41227, CVE-2026-42408, CVE-2026-40435, CVE-2026-40060, CVE-2026-40703, CVE-2026-40701, CVE-2026-28758, CVE-2026-20916, CVE-2026-40423, CVE-2026-41218, CVE-2026-42920, CVE-2026-41957, CVE-2026-40067, CVE-2026-42945)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	BIG-IP (all modules) • 21.0.0 • 17.5.0 - 17.5.1 • 17.1.0 - 17.1.3 • 16.1.0 - 16.1.6 NGINX Open Source • 0.3.50 - 0.9.7 • 1.0.0 - 1.30.0 BIG-IP Next SPK • 2.0.0 - 2.0.2 • 1.7.0 - 1.7.16 BIG-IP Next CNF • 2.0.0 - 2.0.2 • 1.10 - 1.4.0 BIG-IP Next for Kubernetes • 2.0.0 - 2.1.1 NGINX Plus – Versions R32 - R36 BIG-IQ Centralized Management – Versions 8.4.0 - 8.4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/new-updated-articles#f-f5_document_type=Security%20Advisory&aq=%40f5_updated_published_date%20%3E%3D%20now-7d%20OR%20%40f5_original_published_date%20%3E%3D%20now-7d&numberOfResults=50

Affected Product	**Palo Alto Networks**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0265, CVE-2026-0264, CVE-2026-0263, CVE-2026-0262, CVE-2026-0261, CVE-2026-0259, CVE-2026-0258, CVE-2026-0257, CVE-2026-0256, CVE-2026-0251, CVE-2026-0250, CVE-2026-0249, CVE-2026-0248, CVE-2026-0247, CVE-2026-0246, CVE-2026-0245, CVE-2026-0244, CVE-2026-0243, CVE-2026-0242, CVE-2026-0241, CVE-2026-0240, CVE-2026-0239, CVE-2026-0238)
Description	Palo Alto Networks has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Palo Alto Networks advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PAN-OS 12.1 PAN-OS 11.2 PAN-OS 11.1 PAN-OS 10.2 WildFire WF-500 and WF-500-B 12.1.0 WildFire WF-500 and WF-500-B 11.2.0 WildFire WF-500 and WF-500-B 11.1.0 WildFire WF-500 and WF-500-B 10.2.0 Prisma Access Agent Prisma Access 11.2.0 Prisma Access 10.2.0 Prisma Access Agent (Endpoint DLP) Global Protect App GlobalProtect App 6.3 GlobalProtect App 6.2 GlobalProtect App 6.1 GlobalProtect App 6.0 GlobalProtect UWP App 6.3 Prisma SD-WAN ION 6.5 Prisma SD-WAN ION 6.4 Prisma SD-WAN ION 6.3 Trust Protection Foundation 25.3.0 Trust Protection Foundation 25.1.0 Trust Protection Foundation 24.3.0 Trust Protection Foundation 24.1.0 Chronosphere Chronocollector Broker VM 30.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/?sort=-date

Affected Product	**MongoDB**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-8202, CVE-2026-8336, CVE-2026-8201, CVE-2026-8200, CVE-2026-8199, CVE-2026-8053)
Description	MongoDB has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MongoDB Server Versions: • 5.0 affects versions prior to 5.0.33 • 6.0 affects versions prior to 6.0.28 • 7.0 affects versions prior to 7.0.34 • 8.0 affects versions prior to 8.0.23 • 8.2 affects versions prior to 8.2.9 • 8.3 affects versions prior to 8.3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Affected Product	**Drupal**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-8495, CVE-2026-8493, CVE-2026-8492, CVE-2026-8491)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Node View Permissions module version 2.0.0. or prior GTranslate module versions prior to 3.0.5. Colorbox Inline module versions prior to 2.1.1 Date iCal module versions prior to 4.0.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-036 https://www.drupal.org/sa-contrib-2026-035 https://www.drupal.org/sa-contrib-2026-034 https://www.drupal.org/sa-contrib-2026-037

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-10735, CVE-2019-0223, CVE-2022-2996, CVE-2022-48468, CVE-2023-0833, CVE-2024-7254, CVE-2024-9143, CVE-2024-10917, CVE-2024-21208, CVE-2024-21217, CVE-2024-47081, CVE-2024-47535, CVE-2025-1470, CVE-2025-1471, CVE-2025-1948, CVE-2025-2148, CVE-2025-2149, CVE-2025-2900, CVE-2025-4287, CVE-2025-4447, CVE-2025-4565, CVE-2025-5889, CVE-2025-7339, CVE-2025-21587, CVE-2025-24970, CVE-2025-25193, CVE-2025-30698, CVE-2025-46392, CVE-2025-46653, CVE-2025-47273, CVE-2025-47279, CVE-2025-48050, CVE-2025-48734, CVE-2025-49128, CVE-2025-50181, CVE-2025-50182)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. 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 Data System – NPS versions 11.2.0.0 - 11.3.0.2 IBM Watson Knowledge Catalog on-prem versions: • 5.0.0, 5.0.1, 5.0.2, 5.0.3, 5.1.0, 5.1.1, 5.1.2, 5.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7272798 https://www.ibm.com/support/pages/node/7272836

Affected Product	**HP**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2025-20096)
Description	HP has released a security update addressing a vulnerability that exists in their products. **CVE-2025-20096:** Improper input validation in the UEFI firmware for some Intel Reference Platforms may allow an escalation of privilege. System software adversary with a privileged user combined with a high complexity attack may enable data manipulation. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. HP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Windows & Linux BIOS updates: • HP Z4 G5 Workstation • HP Z6 G5 Workstation • HP Z8 G5 Fury Workstation • HP Z8 G5 Workstation
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hp.com/us-en/document/ish_14921729-14921766-16/hpsbhf04116

Affected Product	**cPanel**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43515, CVE-2026-43512, CVE-2026-43514, CVE-2026-43513, CVE-2026-42498, CVE-2026-41293, CVE-2026-41284)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 • ea-tomcat101 version 10.1.54
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/#2559

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.