Advisory Alert

Alert Number: AAA20260910 **Date:** September 10, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
MongoDB	**Critical**	Authorization Bypass Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Check Point	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
HPE	**High**, Medium	Multiple Vulnerabilities
Drupal	**High**, Medium	Multiple Vulnerabilities
cPanel	**High**, Medium, Low	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Palo Alto Networks	**High**, Medium, Low	Multiple Vulnerabilities
MongoDB	**High**, Medium, Low	Multiple Vulnerabilities

Description

Vendor	**MongoDB**
Severity	**Critical**
Affected Vulnerability	Authorization Bypass Vulnerability (CVE-2026-82067)
Description	MongoDB has released a security update addressing a vulnerability that exists in their products. **CVE-2026-82067:** Improper handling of case sensitivity in the configuration validation component of MongoDB Server may cause the authorization subsystem to remain in a default disabled state during server startup. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MongoDB Server: • 8.3.0 affects versions prior to 8.3.9 • 8.0.0 affects versions prior to 8.0.30 • 7.0.0 affects versions prior to 7.0.41
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://jira.mongodb.org/browse/SERVER-131229

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11187, CVE-2025-15467, CVE-2025-15468, CVE-2025-66199, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796)
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 the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Products utilizing: • Intel Management Engine Interface Driver Versions prior to 2613.9.28.0 • Intel Management Engine Components Installer Versions prior to 2613.9.28.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000501815/dsa-2026-203-security-update-for-dell-client-platform-for-multiple-openssl-vulnerabilities

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-40971, CVE-2026-40974, CVE-2026-42579, CVE-2026-47891, CVE-2026-65182, CVE-2026-65637, CVE-2026-65905, CVE-2026-68525, CVE-2026-71290, CVE-2026-58062, CVE-2026-59650, CVE-2026-8763, CVE-2026-42581, CVE-2026-42584, CVE-2026-59083, CVE-2026-59084, CVE-2026-45623, CVE-2026-40976, CVE-2026-41293, CVE-2026-43512, CVE-2026-43515, CVE-2026-47884, CVE-2026-47890)
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	IBM Storage Protect Plus Server versions 10.1.0 to 10.1.19 IBM Storage Protect Plus vSnap versions 10.1.0 to 10.1.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7286752

Vendor	**Check Point**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-85103, CVE-2026-85102)
Description	Check Point has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-85103:** A heap overflow in the VPN certificate ASN.1 decoding flow may allow a remote attacker to remotely execute arbitrary code on the management and Security Gateway. **CVE-2026-85102:** Improper validation of certificate data during VPN negotiation may allow an unauthenticated remote attacker to execute arbitrary code on the Security Gateway. Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Security Gateway - R81 (EOS), R81.10 (EOS), R81.10.X, R81.20, R82, R82.00.X, R82.10 • Security Management Server - R81 (EOS), R81.10 (EOS), R81.10.X, R81.20, R82, R82.00.X, R82.10 • Spark Firewall (Centrally Managed) - R81 (EOS), R81.10 (EOS), R81.10.X, R81.20, R82, R82.00.X, R82.10 • Spark Firewall (Locally Managed) - R81 (EOS), R81.10 (EOS), R81.10.X, R81.20, R82, R82.00.X, R82.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk1000118/ https://support.checkpoint.com/results/sk/sk1000117/

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43493, CVE-2026-53002, CVE-2026-64007, CVE-2026-64563, CVE-2026-68343, CVE-2026-72129, CVE-2026-74480, CVE-2026-6893, CVE-2026-12413, CVE-2026-14164, CVE-2026-14957, CVE-2026-15816, CVE-2026-16313, CVE-2026-50721, CVE-2026-50722)
Description	Red Hat 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. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	RHEL 8 (base) — x86_64, s390x, ppc64le, aarch64 RHEL 8 CodeReady Linux Builder — x86_64, ppc64le, aarch64 RHEL 8.10 — Extended Life Cycle (x86_64, ARM64, ppc64le, s390x) OpenShift Container Platform 4.19 — RHEL 8 & RHEL 9, all four architectures each (x86_64, ppc64le, s390x, aarch64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:66000 https://access.redhat.com/errata/RHSA-2026:63044

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22796, CVE-2024-4741, CVE-2023-6237, CVE-2026-6485, CVE-2026-60001, CVE-2025-29088, CVE-2022-43680, CVE-2023-52425, CVE-2023-52426, CVE-2024-28757, CVE-2026-25210, CVE-2026-32776, CVE-2026-32777, CVE-2026-32778, CVE-2025-60876)
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	Precision 7920 and 7920 XL Rack: • BIOS Versions prior to 2.27.0 • iDRAC9 Firmware Versions prior to 7.00.00.185 Precision 7960 and 7960 XL Rack: • BIOS Versions prior to 2.10.1 • iDRAC9 Versions prior to 7.20.30.54 Dell 14 DC14255 BIOS Versions prior to 1.14.0 Dell 14 Plus 2-in-1 DB04255 BIOS Versions prior to 1.12.0 Dell 14 Plus DB14255 BIOS Versions prior to 1.12.0 Dell 16 DC16256 BIOS Versions prior to 1.11.0 Dell 16 Plus DB16255 BIOS Versions prior to 1.12.0 Dell Pro 14 Essential PV14255 BIOS Versions prior to 1.14.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000501834/dsa-2026-308-security-update-for-dell-precision-rack-bios-for-an-openssl-vulnerability • https://www.dell.com/support/kbdoc/en-us/000501828/dsa-2026-281-security-update-for-dell-client-platform-for-an-insyde-bios-vulnerability • https://www.dell.com/support/kbdoc/en-us/000502809/dsa-2026-390-security-update-for-dell-precision-rack-for-multiple-idrac9-vulnerabilities

Vendor	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-73786, CVE-2026-73787, CVE-2026-73769, CVE-2026-73788, CVE-2026-73789)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE Networking ClearPass Policy Manager: • 6.12.x: ClearPass 6.12.8 and below • 6.11.x: ClearPass 6.11.14 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05130en_us&docLocale=en_US

Vendor	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-87953, CVE-2026-87952, CVE-2026-87951, CVE-2026-87950, CVE-2026-87949, CVE-2026-87948, CVE-2026-87947, CVE-2026-87946, CVE-2026-87945, CVE-2026-87944, CVE-2026-87943, CVE-2026-87940, CVE-2026-87937)
Description	Drupal 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. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SAML SSO - Service Provider module versions prior to 3.2.0 Key auth module versions prior to 2.2.4 Central Authentication System (CAS) Server versions: • prior to 2.0.4 • after and equal to 2.1.0 but prior to 2.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/security

Vendor	**cPanel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-86140, CVE-2026-86138, CVE-2026-86139, CVE-2026-86142, CVE-2026-86143, CVE-2026-86144, CVE-2026-86137, CVE-2026-86141, CVE-2026-80212, CVE-2026-80213)
Description	cPanel 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. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ea-libxml2 version 2.15.3 ea-ruby27 (CentOS 7 and 8 only)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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 Protect Plus Server versions 10.1.0 to 10.1.19 IBM Storage Protect Plus vSnap versions 10.1.0 to 10.1.19 IBM Db2 Bridge All versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7286782 https://www.ibm.com/support/pages/node/7286752

Vendor	**Palo Alto Networks**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0303, CVE-2026-0302, CVE-2026-0304, CVE-2026-0310, CVE-2026-0309, CVE-2026-0308, CVE-2026-0307)
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 the affected systems. Palo Alto Networks advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Checkov by Prisma Cloud 3.2.0 versions prior to 3.2.532 Cortex XDR Broker VM 20.0.96 versions prior to 32.0.52 Cloud NGFW All on Azure and AWS PAN-OS 12.2 versions prior to 12.2.3 PAN-OS 12.1 versions prior to 12.1.4-h10, 12.1.7-h5, 12.1.10 PAN-OS 11.2 versions prior to 11.2.4-h21, 11.2.7-h20, 11.2.10-h14, 11.2.13-h2 PAN-OS 11.1 versions prior to 11.1.4-h36, 11.1.6-h38, 11.1.7-h10, 11.1.10-h33, 11.1.13-h12, 11.1.16-h2 PAN-OS 10.2 versions prior to 10.2.7-h37, 10.2.10-h40, 10.2.13-h24, 10.2.16-h10, 10.2.18-h10 Prisma Access 12.1 versions prior to 12.1.7-h5* Prisma Access 11.2 versions prior to 11.2.7-h20* Prisma Access 10.2 versions prior to 10.2.10-h40* GlobalProtect App All on iOS, Android and ChromeOS GlobalProtect App 6.3 versions prior to: • 6.3.3-h15 on Linux • 6.3.3-h15 on macOS • 6.3.3-h15 on Windows GlobalProtect App 6.2 versions prior to: • 6.2.8-h14 on macOS • 6.2.8-h14 on Windows GlobalProtect App 6.0 versions prior to: • 6.0.15 on Linux • 6.0.15 on macOS • 6.0.15 on Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2026-0303 https://security.paloaltonetworks.com/CVE-2026-0302 https://security.paloaltonetworks.com/CVE-2026-0304 https://security.paloaltonetworks.com/CVE-2026-0310 https://security.paloaltonetworks.com/CVE-2026-0309 https://security.paloaltonetworks.com/CVE-2026-0308 https://security.paloaltonetworks.com/CVE-2026-0307

Vendor	**MongoDB**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-82052, CVE-2026-82053, CVE-2026-82054, CVE-2026-82055, CVE-2026-82056, CVE-2026-82057, CVE-2026-82058, CVE-2026-82059, CVE-2026-82060, CVE-2026-82061, CVE-2026-82062, CVE-2026-82063, CVE-2026-82064, CVE-2026-82065, CVE-2026-82066, CVE-2026-82068, CVE-2026-82069, CVE-2026-82070, CVE-2026-82071, CVE-2026-82073, CVE-2026-82074, CVE-2026-82075, CVE-2026-82076)
Description	MongoDB 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. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MongoDB Server: • 8.3.0 affects versions prior to 8.3.9 • 8.0 affects versions prior to 8.0.30 • 7.0 affects versions prior to 7.0.41
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

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.