Advisory Alert

Alert Number: AAA20260709 **Date:** July 9, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Juniper Networks	**High**, Medium	Multiple Vulnerabilities
Hitachi	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
cPanel	**High**, Medium, Low	Multiple Vulnerabilities
Palo Alto Networks	**High**, Medium, Low	Multiple Vulnerabilities
Drupal	Medium	Access Bypass Vulnerability

Description

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-49844, CVE-2025-46817, CVE-2025-46818, CVE-2025-46819, CVE-2024-25621, CVE-2025-64329, CVE-2026-34714, CVE-2026-35385, CVE-2026-35386, CVE-2026-35387, CVE-2026-35388, CVE-2026-35414, CVE-2026-41293, CVE-2026-43512, CVE-2026-43515, CVE-2026-43513, CVE-2026-41284, CVE-2026-42498, CVE-2026-43514)
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	Dell Enterprise SONiC Distribution versions prior to 4.6.0 Dell Wyse Management Suite Versions WMS 2605 HF1 and prior Dell Wyse Management Suite Repo Versions prior to WMS 2605 HF1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000486907/dsa-2026-290-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000484110/dsa-2026-307

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-71066, CVE-2026-46113, CVE-2026-53359, CVE-2026-46227, CVE-2024-27398, CVE-2024-50125, CVE-2025-68183, CVE-2026-31408, CVE-2026-43027, CVE-2026-43279, CVE-2026-43125, CVE-2026-45984, CVE-2026-46152, CVE-2026-46189, CVE-2026-43074, CVE-2026-43276, CVE-2026-43341, CVE-2026-46155, CVE-2026-46242, CVE-2026-46259)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:36957 • https://access.redhat.com/errata/RHSA-2026:36956 • https://access.redhat.com/errata/RHSA-2026:36767 • https://access.redhat.com/errata/RHSA-2026:36541

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE 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. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	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-20262800-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262799-1/

Vendor	**Juniper Networks**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-57026, CVE-2020-7450, CVE-2026-57025, CVE-2026-57030, CVE-2026-57032, CVE-2026-21901, CVE-2018-1000215, CVE-2022-39836, CVE-2023-27043, CVE-2023-50471, CVE-2023-50472, CVE-2023-51767, CVE-2024-6232, CVE-2024-10963, CVE-2024-41957, CVE-2024-45490, CVE-2026-57028, CVE-2026-57024, CVE-2026-57054, CVE-2025-5914, CVE-2025-48964, CVE-2025-5994, CVE-2025-54389, CVE-2025-47273, CVE-2023-43804, CVE-2023-45803, CVE-2024-37891, CVE-2025-66418, CVE-2025-66471, CVE-2026-21441, CVE-2026-43284, CVE-2026-43500, CVE-2023-53331, CVE-2023-53373, CVE-2024-47081, CVE-2024-52615, CVE-2025-14104, CVE-2025-38556, CVE-2025-38614, CVE-2025-39718, CVE-2025-39730, CVE-2025-39757, CVE-2025-39819, CVE-2025-40909, CVE-2025-5318, CVE-2025-53905, CVE-2025-53906, CVE-2025-5987, CVE-2025-62229, CVE-2025-62230, CVE-2025-62231, CVE-2025-59375, CVE-2025-68973, CVE-2025-61726, CVE-2025-6176, CVE-2025-11561, CVE-2025-64720, CVE-2025-65018, CVE-2025-66293, CVE-2026-22695, CVE-2026-22801, CVE-2026-25646, CVE-2026-0719, CVE-2026-1761, CVE-2025-8176, CVE-2025-9900, CVE-2025-68615, CVE-2025-21605, CVE-2025-46817, CVE-2025-46818, CVE-2025-46819, CVE-2025-49844, CVE-2026-57031, CVE-2026-57021, CVE-2026-33794, CVE-2026-57029, CVE-2026-33803, CVE-2026-33800, CVE-2026-57023, CVE-2026-57019, CVE-2026-57027, CVE-2026-57020, CVE-2026-33802, CVE-2026-33799, CVE-2026-33801, CVE-2026-57022)
Description	Juniper Networks 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. Juniper Networks 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://supportportal.juniper.net/s/global-search/%40uri#sortCriteria=date%20descending&f-sf_primarysourcename=Knowledge&f-sf_articletype=Security%20Advisories&firstResult=20

Vendor	**Hitachi**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54518, CVE-2026-21530, CVE-2026-32161, CVE-2026-32170, CVE-2026-32177, CVE-2026-32209, CVE-2026-33834, CVE-2026-33835, CVE-2026-33837, CVE-2026-33838, CVE-2026-33839, CVE-2026-33841, CVE-2026-34329, CVE-2026-34330, CVE-2026-34331, CVE-2026-34333, CVE-2026-34334, CVE-2026-34336, CVE-2026-34337, CVE-2026-34338, CVE-2026-34339, CVE-2026-34340, CVE-2026-34341, CVE-2026-34342, CVE-2026-34343, CVE-2026-34344, CVE-2026-34345, CVE-2026-34347, CVE-2026-34351, CVE-2026-35415, CVE-2026-35416, CVE-2026-35417, CVE-2026-35418, CVE-2026-35421, CVE-2026-35422, CVE-2026-35423, CVE-2026-35424, CVE-2026-40377, CVE-2026-40380, CVE-2026-40382, CVE-2026-40397, CVE-2026-40398, CVE-2026-40399, CVE-2026-40401, CVE-2026-40403, CVE-2026-40406, CVE-2026-40407, CVE-2026-40408, CVE-2026-40410, CVE-2026-40413, CVE-2026-40414, CVE-2026-40415, CVE-2026-41088, CVE-2026-41097, CVE-2026-42825)
Description	Hitachi 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. Hitachi advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5100, 5200, 5500, 5600, 5100H, 5200H, 5500H and 5600H
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/05.html

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 Verify Identity Access versions 11.0 - 11.0.2 IBM Security Verify Access versions 10.0 - 10.0.9.1 IBM Verify Identity Access Container versions11.0 - 11.0.2 IBM Security Verify Access Container versions 10.0 - 10.0.9.1 IBM Cloud Pak for Applications versions 5.1, 5.2, and 5.3 IBM WebSphere Application Server Liberty versions 17.0.0.3 - 26.0.0.7 CPDS versions 1.0.0.0 - 1.0.10.0 IBM Cloud Pak System: • 2.3.5.0 • 2.3.4.0 • 2.3.4.1 and 2.3.4.1 iFix1 • 2.3.6.0 • 2.3.3.7 and 2.3.3.7 iFix1 • 2.3.3.6, 2.3.3.6 iFix1 and 2.3.3.6 iFix2 IBM WebSphere Application Server versions: • 9.0.0.0 - 9.0.5.28 • 8.5.5.0 - 8.5.5.29
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7279510 • https://www.ibm.com/support/pages/node/7279492 • https://www.ibm.com/support/pages/node/7279367 • https://www.ibm.com/support/pages/node/7279419 • https://www.ibm.com/support/pages/node/7279417 • https://www.ibm.com/support/pages/node/7279377 • https://www.ibm.com/support/pages/node/7279376 • https://www.ibm.com/support/pages/node/7279374 • https://www.ibm.com/support/pages/node/7279371 • https://www.ibm.com/support/pages/node/7253579 • https://www.ibm.com/support/pages/node/7148474 • https://www.ibm.com/support/pages/node/7279554 • https://www.ibm.com/support/pages/node/7279434

Vendor	**cPanel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-14355, CVE-2026-12184, CVE-2026-8286, CVE-2026-8458, CVE-2026-8924, CVE-2026-8926, CVE-2026-8927, CVE-2026-8932, CVE-2026-9079, CVE-2026-9080, CVE-2026-10536, CVE-2026-11564, CVE-2026-11586, CVE-2026-11856, CVE-2026-12064)
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-php82 version 8.2.31 ea-php83 version 8.3.31 ea-php84 version 8.4.22 ea-php85 version 8.5.7 ea-libcurl version 8.17.0-6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Vendor	**Palo Alto Networks**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0288, CVE-2026-0287, CVE-2026-0286, CVE-2026-0285, CVE-2026-0284, CVE-2026-0283, CVE-2026-0282, CVE-2026-0281, CVE-2026-0280, CVE-2026-0279, CVE-2026-0278, CVE-2026-0277, CVE-2026-0276)
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	PAN-OS 12.1 versions: • prior to 12.1.4-h8 • prior to 12.1.7-h2 • prior to 12.1.8 PAN-OS 11.2 versions: • prior to 11.2.4-h20 • prior to 11.2.7-h18 • prior to 11.2.10-h12 • prior to 11.2.13 PAN-OS 11.1 versions: • prior to 11.1.4-h35 • prior to 11.1.6-h35 • prior to 11.1.7-h8 • prior to 11.1.10-h30 • prior to 11.1.13-h9 • prior to 11.1.16 PAN-OS 10.2 versions: • prior to 10.2.7-h36 • prior to 10.2.10-h39 • prior to 10.2.13-h23 • prior to 10.2.16-h9 • prior to 10.2.18-h8 Prisma Access 11.2.0 versions prior to 11.2.7-h18* Prisma Access 10.2.0 versions prior to 10.2.10-h39*
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2026-0288 • https://security.paloaltonetworks.com/CVE-2026-0287 • https://security.paloaltonetworks.com/CVE-2026-0286 • https://security.paloaltonetworks.com/CVE-2026-0285 • https://security.paloaltonetworks.com/CVE-2026-0284 • https://security.paloaltonetworks.com/CVE-2026-0283 • https://security.paloaltonetworks.com/CVE-2026-0282 • https://security.paloaltonetworks.com/CVE-2026-0281 • https://security.paloaltonetworks.com/CVE-2026-0280 • https://security.paloaltonetworks.com/CVE-2026-0279 • https://security.paloaltonetworks.com/CVE-2026-0278 • https://security.paloaltonetworks.com/CVE-2026-0277 • https://security.paloaltonetworks.com/CVE-2026-0276

Vendor	**Drupal**
Severity	**Medium**
Affected Vulnerability	Access Bypass Vulnerability (CVE-2026-15079)
Description	Drupal has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-15079:** The module doesn't sufficiently protect the disabled login form from brute force attacks. Depending on the length of the key this could allow an attacker to use a brute force attack to bypass the protection provided by this module. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	“Login Disable” module versions prior to 2.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-070

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.