Advisory Alert

Alert Number: AAA20260611 **Date:** June 11, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
cPanel	**Critical**	Multiple Vulnerabilities
Red Hat	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Cisco	**High**	Authenticated Privilege Escalation Vulnerability
SUSE	**High**	Multiple Vulnerabilities
MongoDB	**High**, **Medium**	Multiple Vulnerabilities
cPanel	**High**, **Medium**	Multiple Vulnerabilities
Palo Alto Networks	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Drupal	**Medium**	Cross-site scripting (XSS) Vulnerability

Description

Vendor	**cPanel**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42535, CVE-2026-44631, CVE-2026-29167)
Description	cPanel has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-42535:** A path handling issue in mod_dav_fs in Apache 2.4.67 and earlier allows a WebDAV content author to directly manipulate trusted DAV property databases, potentially causing child process crashes. **CVE-2026-44631:** Buffer Underwrite vulnerability in Apache HTTP Server on crafted regular expressions in the configuration. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. **CVE-2026-29167:** Use After Free vulnerability in Apache HTTP Server with mod_ldap in per-directory configuration This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ea-apache24 versions 2.4.67 through 2.4.68
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/#2565

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53781, CVE-2025-21858, CVE-2025-68366, CVE-2026-22984, CVE-2026-22990, CVE-2026-23392, CVE-2026-31581, CVE-2026-31613, CVE-2026-43037, CVE-2026-43038, CVE-2026-43125, CVE-2026-45852, CVE-2026-46181)
Description	Red Hat 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. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:25120

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11187, CVE-2025-15467, CVE-2025-15468, CVE-2025-15469, CVE-2025-66199, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796, CVE-2025-9230)
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 NativeEdge Orchestrator versions prior to 4.2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000475534/dsa-2026-256-security-update-for-dell-native-edge-orchestrator-eo

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-1605, CVE-2026-28367, CVE-2026-28368, CVE-2026-28369, CVE-2026-31532, CVE-2026-31607, CVE-2026-31685, CVE-2026-43163)
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	• JBoss Enterprise Application Platform 8.1 for RHEL 9 x86_64 • JBoss Enterprise Application Platform 8.1 for RHEL 8 x86_64 • JBoss Enterprise Application Platform Text-Only Advisories x86_64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:25126 https://access.redhat.com/errata/RHSA-2026:25125 https://access.redhat.com/errata/RHSA-2026:25095

Vendor	**Cisco**
Severity	**High**
Affected Vulnerability	Authenticated Privilege Escalation Vulnerability (CVE-2026-20245)
Description	Cisco has a security update a vulnerability that exist in their products. **CVE-2026-20245:** 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 Controller Cisco Catalyst SD-WAN Manager Cisco Catalyst SD-WAN Validator
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	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31629, CVE-2026-43037, CVE-2026-43206, CVE-2026-43499, CVE-2026-43501, CVE-2026-45852, CVE-2026-46043, CVE-2026-46243, CVE-2026-31405, CVE-2026-31758, CVE-2026-45970, CVE-2026-46021, CVE-2026-46113)
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	openSUSE Leap 15.5 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262332-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262331-1/

Vendor	**MongoDB**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-9740, CVE-2026-9735, CVE-2026-9754, CVE-2026-9753, CVE-2026-9752, CVE-2026-9751, CVE-2026-9750, CVE-2026-9749, CVE-2026-9748, CVE-2026-9747, CVE-2026-9746, CVE-2026-9743, CVE-2026-9742, CVE-2026-9741)
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 (Multiple Versions) MongoDB affects versions prior to 8.3.3 & 8.2.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Vendor	**cPanel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-29167, CVE-2026-29170, CVE-2026-34355, CVE-2026-34356, CVE-2026-42536, CVE-2026-43951, CVE-2026-44119, CVE-2026-44185, CVE-2026-44186, CVE-2026-48913, CVE-2026-49975)
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-apache24 versions 2.4.67 through 2.4.68
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/#2565

Vendor	**Palo Alto Networks**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0274, CVE-2026-0273, CVE-2026-0272, CVE-2026-0271, CVE-2026-0270, CVE-2026-0269, CVE-2026-0268, CVE-2026-0267, CVE-2026-0266)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2026-0274 https://security.paloaltonetworks.com/CVE-2026-0273 https://security.paloaltonetworks.com/CVE-2026-0272 https://security.paloaltonetworks.com/CVE-2026-0271 https://security.paloaltonetworks.com/CVE-2026-0270 https://security.paloaltonetworks.com/CVE-2026-0269 https://security.paloaltonetworks.com/CVE-2026-0268 https://security.paloaltonetworks.com/CVE-2026-0267 https://security.paloaltonetworks.com/CVE-2026-0266

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-21945, CVE-2026-21932, CVE-2026-21933, CVE-2026-21925, CVE-2025-53066, CVE-2025-53057, CVE-2025-50106, CVE-2025-30749, CVE-2025-30754)
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 Security Verify Directory versions 10.0.0 - 10.0.4 IBM Security Directory Integrator (SDI) versions 7.2.0.0 - 7.2.0.14 & 10.0.0.0 - 10.0.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7275815 https://www.ibm.com/support/pages/node/7275816

Vendor	**Drupal**
Severity	**Medium**
Affected Vulnerability	Cross-site scripting (XSS) Vulnerability (CVE-2026-11908)
Description	Drupal has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-11908:** The Tagify module does not properly sanitise the name of parent taxonomy terms when rendering suggestions in the Tagify dropdown. This results in a cross-site scripting vulnerability that may allow attackers to execute arbitrary JavaScript in the context of the user's session. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Tagify module versions prior to 1.2.52
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-043

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.