Advisory Alert

Alert Number: AAA20260406 **Date:** April 6, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	Improper Access Control Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Drupal	**High**	Authentication Bypass Vulnerability
cPanel	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2026-35616)
Description	Fortinet has released a security update addressing a vulnerability that exists in their FortiClientEMS products. **CVE-2026-35616** - An improper access control vulnerability in Fortinet FortiClientEMS 7.4.5 through 7.4.6 may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiClientEMS 7.4 versions 7.4.5 through 7.4.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-099

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0672, CVE-2026-0865, CVE-2026-0861, CVE-2026-0915, CVE-2026-22695, CVE-2026-22801, CVE-2026-25646, CVE-2026-24882, CVE-2026-22795, CVE-2026-22796, 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-2026-26157, CVE-2026-26158, CVE-2026-23490, CVE-2026-21925, CVE-2026-21932, CVE-2026-21933, CVE-2026-21945, CVE-2025-40257, CVE-2025-40259, CVE-2025-68284, CVE-2025-68285, CVE-2025-68775, CVE-2025-68813, CVE-2025-71085, CVE-2026-22999, CVE-2026-23001, CVE-2026-23010, CVE-2025-5889, CVE-2025-59052, CVE-2024-31573, CVE-2025-41254, CVE-2016-20012, CVE-2020-14145, CVE-2021-28041, CVE-2021-36368, CVE-2023-38408, CVE-2023-48795, CVE-2025-26465, CVE-2025-59419, CVE-2025-11226, CVE-2025-5731, CVE-2026-24400, CVE-2025-68161, CVE-2025-22227, CVE-2024-57699, CVE-2025-48976, CVE-2025-22228, CVE-2025-22235, CVE-2025-41249, CVE-2025-22233, CVE-2025-61795, CVE-2024-12801, CVE-2024-12798 , CVE-2026-28264)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in the third party components utilized by PowerProtect Data Manager 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	Dell PowerProtect Data Manager versions prior to 20.1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000447277/dsa-2026-158-security-update-dell-powerprotect-data-manager-for-multiple-security-vulnerabilities

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-5343)
Description	Drupal has released a security update addressing a vulnerability that exists in a module of their products. **CVE-2026-5343** - The SAML SSO - Service Provider module which allows SAML-protocol-based single-sign-on (SSO) on a Drupal site, doesn't sufficiently block access, leading to an authentication bypass vulnerability. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAML SSO - Service Provider prior to version 3.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-031

Affected Product	**cPanel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-27654, CVE-2026-27784, CVE-2026-32647, CVE-2026-27651, CVE-2026-28753, CVE-2026-28755, CVE-2026-21637, CVE-2026-21710, CVE-2026-21713, CVE-2026-21714, CVE-2026-21717, CVE-2026-21715, CVE-2026-21716, CVE-2026-27135)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in EasyApache 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 version 25.52
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-53066, CVE-2025-53057, CVE-2025-47273, CVE-2025-8715, CVE-2025-8714, CVE-2025-8713, CVE-2025-4207, CVE-2025-13465, CVE-2025-14505, CVE-2024-48949, CVE-2024-48948, CVE-2024-42461, CVE-2024-42460, CVE-2024-42459, CVE-2020-28498, CVE-2025-66471, CVE-2025-66418, CVE-2026-1561, CVE-2025-14915, CVE-2025-14917)
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 WebSphere Application Server - Liberty versions 17.0.0.3 through 26.0.0.3 IBM Storage Scale versions 6.0.0.0 through 6.0.0.1 & 5.2.3.0 through 5.2.3.6 PowerVM VIOS version 4.1.1 & 4.1.2 IBM Security Verify Directory (Container) versions 10.0.0 through 10.0.4 IBM Security Verify Directory versions 10.0.0 through 10.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7268601 https://www.ibm.com/support/pages/node/7268522 https://www.ibm.com/support/pages/node/7268496 https://www.ibm.com/support/pages/node/7268507 https://www.ibm.com/support/pages/node/7267347 https://www.ibm.com/support/pages/node/7267345 https://www.ibm.com/support/pages/node/7267362

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26984, CVE-2025-71238, CVE-2026-23193, CVE-2026-23231, CVE-2025-38109, CVE-2026-23111, CVE-2026-23210, CVE-2026-23231)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:6570 https://access.redhat.com/errata/RHSA-2026:6571

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.