Advisory Alert

Alert Number: AAA202604016 **Date:** April 16, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
cPanel	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
Drupal	**High**, Medium	Multiple Vulnerabilities
Synology	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Cisco	Medium	Multiple Vulnerabilities
ASUS	Medium	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20184, CVE-2026-20147, CVE-2026-20148, CVE-2026-20180, CVE-2026-20186)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ISE 3.5, 3.4, 3.3, 3.2, 3.1 and prior Cisco ISE-PIC 3.5, 3.4, 3.3, 3.2, 3.1 and prior Cisco Webex Services
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-4fverepv • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-traversal-8bYndVrZ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-cui-cert-8jSZYhWL

Affected Product	**cPanel**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-28387, CVE-2026-28388, CVE-2026-28389, CVE-2026-28390)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in the openssl package of their 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	ea-openssl11 package within EasyApache 4 versions prior to 25.54
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23772, CVE-2025-0624, CVE-2025-4945, CVE-2025-11021, CVE-2025-47081, CVE-2025-11561, CVE-2025-5914, CVE-2025-40778, CVE-2025-32990, CVE-2025-6395)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in the third party components of 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	Connectrix Switches and Directors: • SANnav Versions prior to 2.4.0a • Patch for SANnav OVA 2.4.0b Deployment Versions prior to sannav_ova_8xos • Patch for SANnav OVA 3.0.0 Deployment Versions prior to sannav_ova_9x_os_02_2026 • Dell Storage Manager - Replay Manager for Microsoft Servers Versions prior to 8.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000453020/dsa-2026-058-security-update-for-dell-storage-manager-replay-manager-for-microsoft-servers-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000453015/dsa-2026-171-security-update-for-dell-connectrix-b-series-sannav-vulnerabilities

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20585, CVE-2025-54510, CVE-2025-54502)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-20585** – A potential vulnerability that could allow a hypervisor to direct the IOMMU to write into Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) guest memory **CVE-2025-54510** – A vulnerability that could allow a privileged attacker to alter Memory Mapped I/O (MMIO) routing, potentially compromising SEV-SNP integrity on some Zen 5-based products **CVE-2025-54502** - A vulnerability in the AMD processors use of EFI Boot Services which could allow privilege escalation or arbitrary code execution. Lenovo 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://support.lenovo.com/us/en/product_security/LEN-213828

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23269, CVE-2026-23268, CVE-2026-23111, CVE-2025-21780, CVE-2025-21704, CVE-2024-56640, CVE-2024-56593, CVE-2024-56581)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in the kernel component of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu versions 16.04, 18.04, 20.04, 22.04, 24.04 LTS, and 25.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/LSN-0119-1

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6367, CVE-2026-6366, CVE-2026-6365)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-6367** - Drupal 11.3 comes with support for completing entity suggestions whilst adding a link to CKEditor 5. The suggestions aren't sufficiently sanitized and a malicious user could trigger a stored cross site scripting attack against another user. **CVE-2026-6366** - Drupal core contains a chain of methods that could be exploitable when an insecure deserialization vulnerability exists on the site. This so-called "gadget chain" presents no direct threat, but is a vector that can be used to achieve remote code execution or SQL injection if the application deserializes untrusted data due to another vulnerability. **CVE-2026-6365** - Drupal core's jQuery integration for AJAX modal dialog boxes does not sufficiently sanitize certain options, which which can lead to a cross-site scripting (XSS) vulnerability. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal versions: • 8.0.0 through 10.5.8 • 10.6.0 through 10.6.6 • 11.0.0 through 11.2.10 • 11.3.0 through 11.3.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2026-001 https://www.drupal.org/sa-core-2026-002 https://www.drupal.org/sa-core-2026-003

Affected Product	**Synology**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-40530, CVE-2026-4036, CVE-2026-40531, CVE-2026-40532, CVE-2026-40534, CVE-2026-40536, CVE-2026-40537, CVE-2026-40533, CVE-2026-40535, CVE-2026-40538, CVE-2026-40539, CVE-2026-40540)
Description	Synology has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	DSM 7.3 prior to 7.3-81180, 7.3.2-86009-2 DSM 7.2.2 prior to 7.2.2-72806-7 DSM 7.2.1 prior to 7.2.1-69057-10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_26_06 https://www.synology.com/en-global/security/advisory/Synology_SA_26_07

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-8715, CVE-2025-8714, CVE-2025-8713, CVE-2025-4207, CVE-2025-68161, CVE-2025-12183, CVE-2026-1352, CVE-2026-1577, CVE-2026-3676, CVE-2025-14688, CVE-2025-67735, CVE-2025-36122, CVE-2024-5569, CVE-2026-5926)
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 Verify Identity Access Container 11.0 through 11.0.2 IBM Security Verify Access Container 10.0 through 10.0.9.1 IBM Verify Identity Access 11.0 through 11.0.2 IBM Security Verify Access 10.0 through 10.0.9.1 PowerVM VIOS 4.1.1, 4.1.2 IBM Storage Protect Plus Server 10.1 IBM Db2 11.5.0 through 11.5.9, 12.1.0 through 12.1.4 (Client and Server) DB2Connect 11.5.9 SB, 12.1.0 through 12.1.3 SB
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7269372 https://www.ibm.com/support/pages/node/7268496 https://www.ibm.com/support/pages/node/7269511 https://www.ibm.com/support/pages/node/7267642 https://www.ibm.com/support/pages/node/7269426 https://www.ibm.com/support/pages/node/7269424 https://www.ibm.com/support/pages/node/7269435 https://www.ibm.com/support/pages/node/7269434 https://www.ibm.com/support/pages/node/7269433 https://www.ibm.com/support/pages/node/7269432 https://www.ibm.com/support/pages/node/7269429 https://www.ibm.com/support/pages/node/7268496

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20136, CVE-2026-20132, CVE-2026-20161, CVE-2026-20078, CVE-2026-20081, CVE-2026-20059, CVE-2026-20060, CVE-2026-20061, CVE-2026-20152)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in the kernel component of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco AsyncOS Software for Cisco Secure Web Appliance Release 15.2 and prior Cisco Unity Connection 12.5, 14, 15 and prior Cisco ThousandEyes Enterprise Agent Release 1.2 and prior Cisco ISE 3.1, 3.2, 3.3, 3.4, 3.5 and prior Cisco ISE-PIC 3.3, 3.4, 3.5 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-auth-bypass-6YZkTQhd • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-unity-vulns-n2EJSbbw • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-unity-file-download-RmKEVWPx • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-te-agentfilewrite-tqUw3SMU • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-isexss-BS8ctE7U • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-cmd-inj-5WSJcYJB

Affected Product	**ASUS**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-3428, CVE-2026-1880)
Description	ASUS has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-3428** - A Download of Code Without Integrity Check vulnerability in the update modules in ASUS Member Center allows a local user to achieve privilege escalation to Administrator via exploitation of a Time-of-check Time-of-use (TOC-TOU) during the update process, where an unexpected payload is substituted for a legitimate one immediately after download, and subsequently executed with administrative privileges upon user consent. **CVE-2026-1880** - An Incorrect Permission Assignment for Critical Resource vulnerability in the ASUS DriverHub update process allows privilege escalation due to improper protection of required execution resources during the validation phase, permitting a local user to make unprivileged modifications. This allows the altered resource to pass system checks and be executed with elevated privileges upon a user-initiated update ASUS advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ASUS DriverHub 1.0.6.12 and earlier ASUS Member Center 1.6.6.4 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-71238, CVE-2026-23144, CVE-2026-23171, CVE-2026-23204)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel component of their products. These vulnerabilities could be exploited by malicious users to execute privilege escalation and information disclosure exploits. 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 - Extended Update Support 10.0 x86_64, 4 years of updates 10.0 x86_64 • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x, 4 years of updates 10.0 s390x • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le, 4 years of support 10.0 ppc64le • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64, 4 years of updates 10.0 aarch64 • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x • Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:8342

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.