Advisory Alert

Alert Number: AAA20260305 **Date:** March 5, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
cPanel	**High**	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Red Hat	**High**, Medium	Multiple Vulnerabilities
Drupal	**High**, Medium, Low	Multiple Vulnerabilities
NetApp	Medium	Information Disclosure Vulnerability
HPE	Medium	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2025-37184, CVE-2025-37181, CVE-2025-37182, CVE-2025-37183, CVE-2025-37185)
Description	HPE has released security updates multiple vulnerability that exists in their Products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EdgeConnect SD-WAN Orchestrator prior to 9.6.1 EdgeConnect SD-WAN Orchestrator prior to 9.5.6 EdgeConnect SD-WAN Orchestrator prior to 9.4.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04992en_us&docLocale=en_US

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20079, CVE-2026-20131)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their Products. **CVE-2026-20079** - This vulnerability is due to an improper system process that is created at boot time. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute a variety of scripts and commands that allow root access to the device. **CVE-2026-20131** - This vulnerability is due to insecure deserialization of a user-supplied Java byte stream. An attacker could exploit this vulnerability by sending a crafted serialized Java object to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the device and elevate privileges to root. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Security Cloud Control (SCC) Firewall Management Cisco Secure FMC Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2#vp • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh

Affected Product	**cPanel**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-21863, CVE-2025-67733)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-21863 -** A malicious actor with access to the Valkey clusterbus port can send an invalid packet that may cause an out bound read, which might result in the system crashing. The Valkey clusterbus packet processing code does not validate that a clusterbus ping extension packet is located within buffer of the clusterbus packet before attempting to read it. **CVE-2025-67733 -** A malicious user can use scripting commands to inject arbitrary information into the response stream for the given client, potentially corrupting or returning tampered data to other users on the same connection. The error handling code for lua scripts does not properly handle null characters. CPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 (25.49) • ea-valkey72 component's version 7.2.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47599, CVE-2022-48875, CVE-2022-49267, CVE-2024-47659, CVE-2024-49927, CVE-2024-50047, CVE-2024-56548, CVE-2024-56593, CVE-2025-21704, CVE-2025-21726, CVE-2025-22036, CVE-2025-38488, CVE-2025-38561, CVE-2025-39698, CVE-2025-40214, CVE-2025-40215)
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 25.10, 24.04, 22.04, 20.04, 18.04 and 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8070-1 • https://ubuntu.com/security/notices/LSN-0118-1

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir&limit=100#~Vulnerabilities

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37861, CVE-2026-23074)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the Kernel of their products. **CVE-2025-37861 –** Due to a flaw found in the Linux kernel's networking component. A local attacker with low privileges could exploit a design issue in the teql queueing discipline, which is responsible for managing network traffic. By sending specially crafted network packets, an attacker could trigger a use-after-free (UAF) vulnerability; which may lead to a system crash, or potentially allow the attacker to execute unauthorized code or gain elevated system access. **CVE-2026-23074 -** A system crash can occur when two internal threads access the same reply queue during a reset. While the reset process clears the queue and temporarily assigns it an invalid ID (0xFFFF), another thread may attempt to use it and access invalid memory. This can cause the controller to crash and potentially lead to a denial-of-service. 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 9.4 x86_64 • Red Hat Enterprise Linux Server - AUS 9.4 x86_64 • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x • Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x • Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 x86_64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 i386 • Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension (for IBM z Systems) 6 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:3810 https://access.redhat.com/errata/RHSA-2026:3692

Affected Product	**Drupal**
Severity	**High**, **Medium**, **low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-3525, CVE-2026-3526, CVE-2026-3527, CVE-2026-3528, CVE-2026-3529, CVE-2026-3530, CVE-2026-3531, CVE-2026-3532)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to perform Access Bypass, Cross-Site Scripting and Information Disclosure. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenID Connect versions prior to 1.5.0 Google Analytics GA4 module versions prior to 1.1.13 AJAX Dashboard module versions prior to 3.1.0 File access fix module versions prior to 1.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-020 https://www.drupal.org/sa-contrib-2026-021 https://www.drupal.org/sa-contrib-2026-022 https://www.drupal.org/sa-contrib-2026-024 https://www.drupal.org/sa-contrib-2026-025 https://www.drupal.org/sa-contrib-2026-026 https://www.drupal.org/sa-contrib-2026-027

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2026-22052)
Description	NetApp has released security updates addressing a vulnerability that exists in their products. **CVE-2026-22052 -** ONTAP versions 9.12.1 and higher with S3 NAS buckets are susceptible to an information disclosure vulnerability. Successful exploit could allow an authenticated attacker to view a listing of the contents in a directory for which they lack permission. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20260304-0001

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-00212, CVE-2026-00213, CVE-2026-00215, CVE-2026-00214, CVE-2026-00216, CVE-2026-00219)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking • Mobility Conductors • Mobility Controllers • Mobility Gateways (Managed by HPE Aruba Networking Central) • AOS-10 Access Points (AOS-AP) • AOS-8 Instant Access Points (AOS-IAP) Affected Software Version(s): • AOS-10.8.x.x: 10.8.0.0 and below • AOS-10.7.x.x: 10.7.2.2 and below • AOS-10.4.x.x: 10.4.1.10 and below • AOS-8.13.x.x: 8.13.1.1 and below • AOS-8.12.x.x: 8.12.0.6 and below • AOS-8.10.x.x: 8.10.0.21 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05026en_us&docLocale=en_US

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.