TLP: WHITE

Advisory Alert

Alert Number: AAA20260122 **Date:** January 22, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Remote Code Execution Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
HPE	**Medium**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42394, CVE-2024-42395, CVE-2024-42393)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their Products. **CVE-2024-42393 -** An unauthenticated stack-based buffer overflow in the Aruba "Soft AP Daemon" PAPI service that can allow a remote attacker to execute arbitrary code, leading to complete system compromise without authentication. **CVE-2024-42394 -** Another unauthenticated RCE buffer overflow in the same Soft AP PAPI service affecting ArubaOS/AOS-Instant platforms; exploitation may let attackers run arbitrary commands with full system control. **CVE-2024-42395 -** A similar unauthenticated buffer overflow in the Aruba AP Certificate Management Service via PAPI, enabling remote attackers to execute arbitrary OS-level code, potentially fully compromising the affected access point. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	AOS-10 AP 10.6.x.x: 10.6.0.0 and below AOS-10 AP 10.4.x.x: 10.4.1.3 and below AOS-8 Instant 8.12.x.x: 8.12.0.1 and below AOS-8 Instant 8.10.x.x: 8.10.0.12 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-20045)
Description	Cisco has released a security update addressing a vulnerability that exists in their Products. **CVE-2026-20045 –** Due to improper validation of user-supplied input in HTTP requests processed by the web-based management interface. An attacker can send specially crafted HTTP requests to trigger execution of arbitrary commands on the underlying operating system. Successful exploitation could allow an unauthenticated, remote attacker to gain user-level access and then elevate privileges to root, leading to complete system compromise of the affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Unified CM Unified CM SME Unified CM IM&P Unity Connection Webex Calling Dedicated Instance
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50233, CVE-2022-50327, CVE-2022-50367, CVE-2022-50409, CVE-2022-50490, CVE-2023-53676, CVE-2023-53717, CVE-2024-58239, CVE-2025-38476, CVE-2025-38572, CVE-2025-38608, CVE-2025-39682, CVE-2025-40204)
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4 openSUSE Leap 15.5 openSUSE Leap 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20260191-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260200-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260203-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260204-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260202-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260206-1/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Third-party components in their Dell networking 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 Networking OS10 versions prior to 10.6.0.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000417961/dsa-2026-034-security-update-for-dell-networking-os10-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21724, CVE-2025-37849, CVE-2025-37891, CVE-2025-40154, CVE-2025-40277)
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 - 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:0917

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51385, CVE-2023-48795, CVE-2024-42400, CVE-2024-42396, CVE-2024-42399, CVE-2024-42398, CVE-2024-42397)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to perform remote code execution and Denial of Service (DoS) attacks. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	AOS-10 AP 10.6.x.x: 10.6.0.0 and below AOS-10 AP 10.4.x.x: 10.4.1.3 and below AOS-8 Instant 8.12.x.x: 8.12.0.1 and below AOS-8 Instant 8.10.x.x: 8.10.0.12 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20055, CVE-2026-20109, CVE-2026-20092, CVE-2026-20080)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to in order execute Cross-site scripting, privilege escalation, and Denial of Service (DoS) attacks. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Packaged Contact Center Enterprise (PCCE) Cisco Unified Contact Center Enterprise (Unified CCE) Cisco Intersight Virtual Appliance Cisco IEC6400 Wireless Backhaul Edge Compute Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iec6400-Pem5uQ7v • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-intersight-privesc-p6tBm6jk • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucce-pcce-xss-2JVyg3uD

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.