



Advisory Alert

Alert Number: **AAA20261001** Date: October 1, 2026

Document Classification Level : **Public Circulation Permitted | Public**

Information Classification Level : **TLP: WHITE**

Overview

Vendor	Severity	Vulnerability
Cisco	Critical	Authentication Bypass Vulnerability
WatchGuard	High	Security Update
Red Hat	High, Medium	Multiple Vulnerabilities
cPanel	High, Medium, Low	Multiple Vulnerabilities

Description

Vendor	Cisco
Severity	Critical
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-76504)
Description	Cisco has released a security update addressing a vulnerability that exists in their products. CVE-2026-76504: This vulnerability is due to improper handling of URI encoding in an HTTP request, which allows the request to bypass an authentication rule that is intended to restrict access to a specific API endpoint. An attacker could exploit this vulnerability by sending a crafted HTTP request to the API of the affected system. A successful exploit could allow the attacker to bypass authentication and gain access to the API as the admin user Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Catalyst SD-WAN Manager versions: - Earlier than 20.9 20.9 20.12 20.15 20.18 26.1 26.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU

Vendor	WatchGuard
Severity	High
Affected Vulnerability	Security Update (CVE-2026-86134)
Description	WatchGuard has released a security update addressing a vulnerability that exists in their products. CVE-2026-86134: A NULL pointer dereference vulnerability in the WatchGuard Fireware OS authentication process allows a remote, unauthenticated attacker to crash the management daemon by sending a specially request to the login interface, resulting in a denial of service. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Fireware OS (Default): 2026.3 up to but not including 2026.3.2 2025.0 up to but not including 2026.2.3 12.0 up to but not including 12.12.3 Fireware OS (All Platforms): 12.0 up to but not including 12.5.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/CVE-2026-86134/

Vendor	Red Hat
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49670, CVE-2024-57990, CVE-2026-31663, CVE-2026-43493, CVE-2026-52924, CVE-2026-52993, CVE-2026-53002, CVE-2026-53091, CVE-2026-53239, CVE-2026-63917, CVE-2026-63919, CVE-2026-63921, CVE-2026-64558, CVE-2026-68294, CVE-2026-68426, CVE-2026-68480, CVE-2026-72098, CVE-2026-74746, CVE-2026-64102, CVE-2026-68299, CVE-2026-72099, CVE-2026-72329, CVE-2026-56853, CVE-2026-56858, CVE-2026-56859, CVE-2026-56860, CVE-2026-56862, CVE-2026-33814, CVE-2026-39829, CVE-2026-27727, CVE-2026-27830, CVE-2026-42578, CVE-2026-42581, CVE-2026-42583, CVE-2026-42584, CVE-2026-42585, CVE-2026-54369, CVE-2026-60002, CVE-2025-39964, CVE-2026-68121, CVE-2026-74469, CVE-2026-74581, CVE-2026-81000)
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	Red Hat Enterprise Linux 10 Base: - Base (aarch64) Red Hat Enterprise Linux 9.6: 4 Years of Updates (aarch64, s390x) - Advanced Update Support (AUS) (x86_64) - CodeReady Linux Builder - Extended Update Support (aarch64, ppc64le, s390x, x86_64) - Extended Update Support (EUS) (aarch64, ppc64le, s390x, x86_64) - Extended Life Cycle (ELC) (aarch64, ppc64le, s390x, x86_64) - Update Services for SAP Solutions (E4S) (ppc64le, x86_64) Red Hat Enterprise Linux 8 Base & 8.10: - Base & CodeReady Linux Builder 8 (aarch64, ppc64le, s390x, x86_64) - Extended Life Cycle (ELC) 8.10 (aarch64, ppc64le, s390x, x86_64) Red Hat OpenShift: - OpenShift Container Platform - OpenShift File Integrity Operator (FIO) - OpenShift Container Platform 4.19: - RHEL 9 Base (aarch64, ppc64le, s390x, x86_64) - RHEL 8 Base (aarch64, ppc64le, s390x, x86_64) Red Hat Middleware & Application Platforms: - JBoss Enterprise Application Platform 7.1 EUS (x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:74174 https://access.redhat.com/errata/RHSA-2026:74133 https://access.redhat.com/errata/RHSA-2026:74025 https://access.redhat.com/errata/RHSA-2026:74023 https://access.redhat.com/errata/RHSA-2026:73976 https://access.redhat.com/errata/RHSA-2026:71440 https://access.redhat.com/errata/RHSA-2026:73788

Vendor	cPanel
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-1218, CVE-2025-14181, CVE-2026-6103, CVE-2026-17545, CVE-2026-91765, CVE-2026-91766, CVE-2026-91767, CVE-2026-91768, CVE-2026-91769, CVE-2026-92842, CVE-2026-93682)
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-php82 version 8.2.33 ea-php83 version 8.3.33 ea-php84 version 8.4.25 ea-php85 version 8.5.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

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.