



Advisory Alert

Alert Number: **AAA20261005** Date: October 5, 2026

Document Classification Level : **Public Circulation Permitted | Public**
Information Classification Level : **TLP: WHITE**

Overview

Vendor	Severity	Vulnerability
IBM	Critical	Multiple Vulnerabilities
HP	Critical	Multiple Vulnerabilities
Red Hat	High	Multiple Vulnerabilities
Citrix	High	Memory Overflow Vulnerability
IBM	High, Medium, Low	Multiple Vulnerabilities
Ubuntu	High, Medium, Low	Multiple Vulnerabilities
cPanel	Medium, Low	Multiple Vulnerabilities

Description

Vendor	IBM
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-39832, CVE-2026-42508, CVE-2026-43114, CVE-2026-52924, CVE-2026-53131, CVE-2026-74581, CVE-2026-6653, CVE-2026-63888, CVE-2026-64007, CVE-2026-64386, CVE-2026-68343, CVE-2026-68388, CVE-2026-52993, CVE-2026-64530, CVE-2026-53006, CVE-2026-55203, CVE-2026-43198, CVE-2026-5450, CVE-2026-43038, CVE-2026-45898, CVE-2026-44432, CVE-2026-46155, CVE-2026-46244, CVE-2026-46316, CVE-2026-31669, CVE-2026-43414, CVE-2026-46135, CVE-2025-68741, CVE-2026-31402, CVE-2026-31607, CVE-2025-14087, CVE-2026-60002, CVE-2026-23455, CVE-2026-31685, CVE-2025-68121)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security Verify Access (Base & Docker) versions 10.0 to 10.0.9.2 IBM Verify Identity Access (Base & Docker) versions 11.0 to 11.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7290794

Vendor	HP
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities
Description	HP 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. HP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HP ThinPro versions: - prior to HP ThinPro 9 SP3 - prior to HP ThinPro 8.1 SP10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hp.com/us-en/document/ish_15736095-15736118-16/hpsbhf04154 https://support.hp.com/us-en/document/ish_15735991-15736015-16/hpsbhf04155

Vendor	Red Hat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22984, CVE-2026-31467, CVE-2026-31663, CVE-2026-31581, CVE-2026-43493, CVE-2026-52993, CVE-2026-53239, CVE-2026-63921, CVE-2026-63919, CVE-2026-63917, CVE-2026-64017, CVE-2026-64191, CVE-2026-64438, CVE-2026-64368, CVE-2026-68294, CVE-2026-68426, CVE-2026-72130, CVE-2026-72098, CVE-2026-74746, CVE-2026-80844)
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 10.0: 4 Years of Updates / Support (aarch64, ppc64le, s390x, x86_64) - CodeReady Linux Builder - Extended Update Support (aarch64, ppc64le, s390x, x86_64) - Extended Update Support (EUS) (aarch64, ppc64le, s390x, x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:75560 https://access.redhat.com/errata/RHSA-2026:74974

Vendor	Citrix
Severity	High
Affected Vulnerability	Memory Overflow Vulnerability (CVE-2026-88779)
Description	Citrix has released a security update addressing a vulnerability that exists in their products. CVE-2026-88779: Memory overflow vulnerability leading to Denial of Service Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Citrix NetScaler ADC and Citrix NetScaler Gateway 14.1 BEFORE 14.1-73.41 Citrix NetScaler ADC and Citrix NetScaler Gateway 13.1 BEFORE 13.1-64.28 Citrix NetScaler ADC FIPS BEFORE 14.1-73.41 FIPS Citrix NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.282
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697174&articleURL=Citrix_NetScaler_ADC_and_Citrix_NetScaler_Gateway_Security_Bulletin_for_CVE_2026_88779

Vendor	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security Verify Access (Base & Docker) versions 10.0 to 10.0.9.2 IBM Verify Identity Access (Base & Docker) versions 11.0 to 11.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7290794

Vendor	Ubuntu
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 14.04, 16.04, 22.04, 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8864-1 https://ubuntu.com/security/notices/USN-8816-4 https://ubuntu.com/security/notices/USN-8818-6

Vendor	cPanel
Severity	Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42356, CVE-2026-42528, CVE-2026-46729, CVE-2026-47360, CVE-2026-48005, CVE-2026-56153, CVE-2026-56154, CVE-2026-56449, CVE-2026-57941, CVE-2026-58415, CVE-2026-59685, CVE-2026-59797, CVE-2026-63045, CVE-2026-63292, CVE-2026-63686, CVE-2026-63718, CVE-2026-73636, CVE-2026-73637, CVE-2026-79768, CVE-2026-93546)
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-apache24 versions 2.4.68
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.