Advisory Alert

Alert Number: AAA20261113 **Date:** November 13, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
cPanel	**Critical**	Race Condition Vulnerability
Citrix	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
PostgreSQL	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Citrix	**High**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Low**	Multiple Vulnerabilities
cPanel	**Low**	Buffer Overflow Vulnerability

Description

Vendor	**cPanel**
Severity	**Critical**
Affected Vulnerability	Race Condition Vulnerability (CVE-2026-119618)
Description	cPanel has released a security update addressing a vulnerability that exists in their products. **CVE-2026-119618:** Concurrent Execution using Shared Resource with Improper Synchronization vulnerability in Apache HTTP Server's mod_http2 in assign_headers() can lead to RCE. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.70. Affected releases of mod_h2 from GitHub: from 2.0.8 through 2.0.42. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ea-apache24 Versions prior to 2.4.71
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Vendor	**Citrix**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-120868, CVE-2026-107407, CVE-2026-107408, CVE-2026-107409, CVE-2026-107410, CVE-2026-107411, CVE-2026-107412, CVE-2026-107413, CVE-2026-120869)
Description	Citrix 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. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Citrix NetScaler Console 14.1 BEFORE 14.1-74.34 • Citrix NetScaler ADC and Citrix NetScaler Gateway 14.1 BEFORE 14.1-73.57 • Citrix NetScaler ADC and Citrix NetScaler Gateway 13.1 BEFORE 13.1-64.39 • Citrix NetScaler ADC FIPS BEFORE 14.1-73.58 FIPS • Citrix NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.293
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697305&articleURL=Citrix_NetScaler_ADC_and_Citrix_NetScaler_Gateway_Security_Bulletin • https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697320&articleURL=Citrix_NetScaler_Console_Security_Bulletin_for_CVE_2026_120869

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-64534, CVE-2026-31709, CVE-2026-53361, CVE-2026-74705, 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 for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.6 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.6 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:99630 • https://access.redhat.com/errata/RHSA-2026:99722

Vendor	**PostgreSQL**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6460, CVE-2026-6467, CVE-2026-14661, CVE-2026-16237, CVE-2026-16240, CVE-2026-18447, CVE-2026-116303, CVE-2026-116304, CVE-2026-116306, CVE-2026-116307, CVE-2026-116308, CVE-2026-116309, CVE-2026-116310, CVE-2026-116311, CVE-2026-116312, CVE-2026-116313, CVE-2026-116314, CVE-2026-116315, CVE-2026-116316, CVE-2026-116317, CVE-2026-116318, CVE-2026-116319, CVE-2026-116320, CVE-2026-116321, CVE-2026-116322, CVE-2026-116323, CVE-2026-116325, CVE-2026-116326, CVE-2026-116327, CVE-2026-116328, CVE-2026-116329, CVE-2026-116330, CVE-2026-116331, CVE-2026-116332, CVE-2026-116333, CVE-2026-116335, CVE-2026-116336, CVE-2026-120139, CVE-2026-120141, CVE-2026-120142, CVE-2026-120143, CVE-2026-120144, CVE-2026-120145, CVE-2026-120146, CVE-2026-120147, CVE-2026-120148, CVE-2026-120149, CVE-2026-120150, CVE-2026-120151, CVE-2026-120152, CVE-2026-120153, CVE-2026-120154)
Description	PostgreSQL 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. PostgreSQL advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PostgreSQL Core Server, Contrib Module & Client Versions: • 18 • 17 • 16 • 15 • 14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.postgresql.org/support/security/

Vendor	**Citrix**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-107414, CVE-2026-107415, CVE-2026-111340, CVE-2026-111341, CVE-2026-111342, CVE-2026-111343, CVE-2026-111344, CVE-2026-111345, CVE-2026-111346, CVE-2026-111347, CVE-2026-111348, CVE-2026-111349, CVE-2026-120860, CVE-2026-120861, CVE-2026-120862, CVE-2026-120863, CVE-2026-120864, CVE-2026-120865, CVE-2026-120866, CVE-2026-120867, CVE-2026-118268, CVE-2026-118269)
Description	Citrix 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. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Citrix NetScaler ADC and Citrix NetScaler Gateway 14.1 BEFORE 14.1-73.57 • Citrix NetScaler ADC and Citrix NetScaler Gateway 13.1 BEFORE 13.1-64.39 • Citrix NetScaler ADC FIPS BEFORE 14.1-73.58 FIPS • Citrix NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.293 • Citrix Secure Access Client for Linux versions BEFORE 26.10.4 • Citrix Secure Access Client for Windows versions BEFORE 26.11.1.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697305&articleURL=Citrix_NetScaler_ADC_and_Citrix_NetScaler_Gateway_Security_Bulletin • https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697281&articleURL=Citrix_Secure_Access_Client_for_Linux_Security_Bulletin_for_CVE_2026_118269 • https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697280&articleURL=Citrix_Secure_Access_Client_for_Windows_Security_Bulletin_for_CVE_2026_118268

Vendor	**IBM**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-86140, CVE-2026-86141, CVE-2026-86143, CVE-2026-86144)
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	• AIX Version - 7.2 • AIX Versions - 7.3 • VIOS Versions - 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7293277

Vendor	**cPanel**
Severity	**Low**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-109163)
Description	cPanel has released a security update addressing a vulnerability that exists in their products. **CVE-2026-109163:** Stack-based buffer overflow vulnerability in Apache HTTP Server's mod_vhost_alias (after CVE-2026-63292) This issue affects Apache HTTP Server: 2.4.69. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ea-apache24 Versions prior to 2.4.71
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.