

CVE-2026-41940

WebPros cPanel & WHM and WP2 (WordPress Squared) Missing Authentication for Critical Function Vulnerability

Exigent

CISA KEV since Apr 30, 2026

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

cPanel and WHM versions after 11.40 contain an authentication bypass vulnerability in the login flow that allows unauthenticated remote attackers to gain unauthorized access to the control panel.

EVRS

95/100

Immediate priority

CVSS V4.0

9.3

Critical · NVD

EPSS

0.985

99.92nd percentile · FIRST

CISA DEADLINE

May 3, 2026

CISA federal deadline · Overdue by 6 months

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.985 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
cpanel	≥ 11.40 < 86.0.41 ≥ 88.0.0 < 110.0.97 ≥ 112.0.0 < 118.0.63 ≥ 120.0.0 < 124.0.35 ≥ 126.0.1 < 126.0.54 ≥ 128.0.0 < 130.0.19 ≥ 132.0.0 < 132.0.29 ≥ 134.0.0 < 134.0.20 ≥ 136.0.0 < 136.0.5	86.0.41 · 110.0.97 · 118.0.63 · 124.0.35 · 126.0.54 · 130.0.19	NVD
whm	≥ 11.40 < 86.0.41 ≥ 88.0.0 < 110.0.97 ≥ 112.0.0 < 118.0.63 ≥ 120.0.0 < 124.0.35 ≥ 126.0.1 < 126.0.54 ≥ 128.0.0 < 130.0.19 ≥ 132.0.0 < 132.0.29 ≥ 134.0.0 < 134.0.20 ≥ 136.0.0 < 136.0.5	no fixed version listed	NVD
wp squared	< 136.1.7	no fixed version listed	NVD



Sources

Vendor guidance	github.com/advisories/GHSA-85qr-8rxc-62gv	Additional guidance	support.cpanel.net/hc/en-us/articles/40073787579671-cPanel-WHM-Security-Update-04-28-2026
docs.cpanel.net	docs.cpanel.net/release-notes/release-notes/	docs.wpsquared.com	docs.wpsquared.com/changelogs/versions/changelog/#13617
nvd.nist.gov	nvd.nist.gov/vuln/detail/CVE-2026-41940	NVD	nvd.nist.gov/vuln/detail/CVE-2026-41940
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-26246
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-41940		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.