INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-29 18:48 UTC

CVE-2026-41940: Critical Authentication Bypass in cPanel/WHM Requires Manual Emergency Patch

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0094
Type	CVE Vulnerability
CVE ID	CVE-2026-41940
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	cPanel versions prior to 11.110.0.97, 11.118.0.63, 11.126.0.54, 11.132.0.29, 11.136.0.5, 11.134.0.20; WHM (WebHost Manager), WebPros International
Published	2026-04-29T11:51:44
Discovery Source	Rss

Executive Summary

A critical authentication bypass vulnerability (CVE-2026-41940, CVSS 9.5) affects all supported versions of cPanel and WHM, the hosting control panel software used by a substantial portion of the global web hosting industry. An unauthenticated attacker can gain full control of individual hosting accounts or entire server environments without valid credentials. WebPros International has issued an emergency out-of-band patch, but it requires manual deployment, meaning thousands of hosting providers and the websites they serve remain exposed until administrators act.

Technical Analysis

CVE-2026-41940 is an authentication bypass vulnerability in cPanel and WHM (WebPros International) with a CVSS base score of 9.5. Root causes are classified under CWE-287 (Improper Authentication), CWE-288 (Authentication Bypass Using an Alternate Path or Channel), and CWE-306 (Missing Authentication for Critical Function). No authentication is required for exploitation. Depending on which panel interface is targeted, a successful exploit yields full hosting account takeover or complete WHM server administration. Affected versions: cPanel/WHM prior to 11.110.0.97, 11.118.0.63, 11.126.0.54, 11.132.0.29, 11.134.0.20, 11.136.0.5. WebPros has released an emergency out-of-band patch; no automated update path is confirmed, requiring manual application by server administrators. Active exploitation in the wild is not yet confirmed; confidence in exploitation risk is medium based on vulnerability severity and attack surface. MITRE ATT&CK techniques

associated with likely post-exploitation activity include T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1098 (Account Manipulation), T1078 (Valid Accounts), T1133 (External Remote Services), T1056.001 (Keylogging), T1071 (Application Layer Protocol), and T1583.006 (Web Services). Sources: NVD (T1), BleepingComputer (T3), watchTowr (T3).

Action Checklist

1. Step 1: Containment, Immediately restrict external access to cPanel (port 2082/2083) and WHM (port 2086/2087) interfaces at the firewall or WAF level for all servers not yet patched. Limit access to trusted management IP ranges only. Do not expose these interfaces to the open internet during the patch window.
2. Step 2: Detection, Audit server access logs for cPanel and WHM interfaces for anomalous unauthenticated requests or unexpected session initiations, particularly those that succeeded without valid credential exchange. On Linux-based cPanel installations, typical log locations include /usr/local/cpanel/logs/access_log and /usr/local/cpanel/logs/login_log (paths may vary by deployment; consult cPanel documentation for your version). Review authentication events for missing credential validation steps. Check for newly created cPanel accounts, SSH keys, or elevated WHM users not tied to known provisioning activity.
3. Step 3: Eradication, Apply the emergency out-of-band patch issued by WebPros International manually to all affected cPanel/WHM servers. Target patched versions: 11.110.0.97, 11.118.0.63, 11.126.0.54, 11.132.0.29, 11.134.0.20, or 11.136.0.5 depending on your release tier. Consult the WebPros security advisory directly for the patch delivery mechanism; no automated update path is confirmed at analysis time.
4. Step 4: Recovery, After patching, verify installed cPanel/WHM version matches a patched release. Audit all hosting accounts and WHM administrator accounts for unauthorized additions, permission changes, or backdoor mechanisms (web shells, unauthorized SSH keys, modified .htaccess files). Re-enable external interface access only after patch verification is complete and anomalous accounts are purged.
5. Step 5: Post-Incident, Review your patch deployment process for shared hosting infrastructure and establish a manual emergency patch SLA given the absence of an automated update path. Evaluate whether cPanel and WHM administrative interfaces should be routinely accessible from the public internet or restricted to management VPNs as a standing control. Map control gaps to CIS Benchmark recommendations for hosting panel hardening.

Detection Guidance

Focus detection on cPanel (ports 2082/2083) and WHM (ports 2086/2087) access logs. Key log paths on Linux deployments typically include /usr/local/cpanel/logs/access_log (cPanel interface requests), /usr/local/cpanel/logs/login_log (authentication events), and /usr/local/cpanel/logs/error_log (deployment paths may vary; consult cPanel documentation). Hunt for HTTP 200 or 302 responses on authenticated endpoints preceded by requests that contain no credential submission, a pattern consistent with authentication bypass rather than valid login. Look for account creation events (WHM account creation API calls, new cPanel user provisioning) that do not correlate with known administrative sessions. Post-exploitation indicators aligned to T1505.003 include newly written .php files in public_html directories and unexpected cron job additions. T1098 indicators include new SSH authorized_keys entries and WHM reseller privilege escalations. No public IOCs

(IPs, hashes, domains) are confirmed at analysis time. Confidence in active exploitation in the wild is MEDIUM.

Framework Mappings

MITRE-ATTACK

- **T1583.006** — Web Services
- **T1190** — Exploit Public-Facing Application
- **T1071** — Application Layer Protocol
- **T1056.001** — Keylogging
- **T1505.003** — Web Shell
- **T1098** — Account Manipulation
- **T1078** — Valid Accounts
- **T1133** — External Remote Services

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SI-4** — System Monitoring
- **CM-2** — Baseline Configuration
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access

- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1583.006	Web Services	Resource-Development
T1190	Exploit Public-Facing Application	Initial-Access
T1071	Application Layer Protocol	Command-And-Control
T1056.001	Keylogging	Collection
T1505.003	Web Shell	Persistence
T1098	Account Manipulation	Persistence
T1078	Valid Accounts	Defense-Evasion
T1133	External Remote Services	Persistence

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/cpanel-whm-emergency...	T3
CVE-2026-41940 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-41940	T1
CVE-2026-41940 | Tenable®	https://www.tenable.com/cve/CVE-2026-41940	T3

Source	URL	Tier
cPanel Authentication Bypass CVE-2026-41940 - watchTowr	https://watchtowr.com/resources/2765-rapid-reaction-cpanel-authenti...	T3
r/netsec on Reddit: The Internet Is Falling Down, Falling Down ...	https://www.reddit.com/r/netsec/comments/1sz5aoi/the_internet_is_fa...	T3

Generated 2026-04-29 18:48 UTC by TJS Security Command Center