INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-29 18:49 UTC

cPanel Authentication Bypass Affects All Supported Versions, Emergency Patches Released, Ports 2083/2087 at Risk

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0095
Type	CVE Vulnerability
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; hosting providers including Namecheap running unpatched cPanel infrastructure
Published	2026-04-29T05:37:00
Discovery Source	Rss

Executive Summary

A critical authentication bypass vulnerability affects multiple active branches of cPanel and WHM (versions prior to 11.110.0.97, 11.118.0.63, 11.126.0.54, 11.132.0.29, 11.134.0.20, and 11.136.0.5), allowing unauthenticated attackers to gain full administrative access to web hosting control panels without valid credentials. Active exploitation has been reported, making this an immediate patching emergency for any organization running cPanel or WHM infrastructure. As of the audit date, cPanel has not requested a CVE identifier despite active exploitation, indicating emergency patch prioritization over formal CVE workflow. The business risk is severe: successful exploitation grants attackers complete control over hosted websites, email systems, databases, and customer data across shared, VPS, and dedicated hosting environments.

Technical Analysis

An authentication bypass vulnerability affects multiple active branches of cPanel and WHM prior to the following patched releases: 11.110.0.97, 11.118.0.63, 11.126.0.54, 11.132.0.29, 11.134.0.20, and 11.136.0.5. As of the audit date, cPanel has not requested or received a CVE identifier despite active exploitation, indicating emergency patch prioritization over formal CVE workflow. The vulnerability maps to CWE-287 (Improper Authentication), CWE-306 (Missing Authentication for Critical Function), and CWE-303 (Incorrect Implementation of Authentication Algorithm). Attack surface is exposed on port 2083 (cPanel user interface) and

port 2087 (WHM administrative interface). Unauthenticated remote attackers can bypass authentication controls to gain full control panel access. MITRE ATT&CK techniques implicated include T1133 (External Remote Services), T1190 (Exploit Public-Facing Application), T1556 (Modify Authentication Process), and T1021 (Remote Services). Active exploitation has been reported by multiple security sources. No CVSS vector or EPSS data has been published as of this writing. cPanel has released emergency patches across six active version branches. Compensating controls implemented by some hosting providers (e.g., InMotion Hosting) include firewall-level restrictions on ports 2083 and 2087. Technical exploit details have not been publicly disclosed by cPanel. No threat actor attribution has been established.

Action Checklist

1. Step 1: Containment, immediately restrict inbound access to ports 2083 and 2087 at the firewall or network perimeter for all internet-facing cPanel/WHM servers; allow access only from known administrative IP ranges as a compensating control while patching proceeds.
2. Step 2: Detection, audit current cPanel/WHM version across all managed servers. Review authentication logs on ports 2083 and 2087 for anomalous access attempts, successful logins from unrecognized IPs, or login events that lack preceding authentication challenge entries. If you have direct server access, check logs typically located at /usr/local/cpanel/logs/access_log and /var/log/cpanel/login_log (note: paths vary by provider and configuration). If you use a managed hosting provider, request access log exports for the exposure window from their support team. Look for unexpected account creation or privilege changes in WHM audit logs.
3. Step 3: Eradication, apply cPanel emergency patches immediately; target versions are 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 active branch; update via WHM >> cPanel >> Update Preferences or the command-line updater (/usr/local/cpanel/scripts/upcp).
4. Step 4: Recovery, after patching, verify installed version against the patched release list; re-enable port access only after version confirmation; audit all WHM and cPanel accounts for unauthorized changes, new accounts, modified SSH keys, altered DNS records, or added email forwarders that may indicate exploitation during the exposure window.
5. Step 5: Post-Incident, evaluate whether cPanel administrative interfaces should ever be internet-facing without VPN or IP allowlisting; implement continuous version monitoring for cPanel/WHM to reduce time-to-patch on future emergency advisories; review hosting provider SLAs and patch notification channels to ensure emergency advisories reach the patching team within hours, not days.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and potentially regulatory bodies if forensic analysis of /var/cpanel/accounting.log, cpanel-login.log, or authorized_keys files reveals successful unauthorized access during the exposure window on servers hosting PII, PHI, or payment card data — as this would trigger breach notification obligations under applicable regulations (GDPR 72-hour window, HIPAA 60-day window, PCI DSS Requirement 12.10).

Recovery Notes	After patching, maintain firewall restrictions on ports 2083/2087 for a minimum of 72 hours post-patch while completing the full account audit, as attackers who achieved access via the authentication bypass may have implanted backdoors (SSH keys, malicious cron jobs, web shells under /home/*/public_html/) that persist independently of the cPanel vulnerability. Monitor `/var/log/secure`, `/var/log/auth.log`, and web server access logs (Apache: `/usr/local/apache/logs/access_log`) for 30 days post-incident for signs of re-access via implanted credentials. Verify DNS record integrity for all hosted domains daily for two weeks, as DNS hijacking is a high-probability post-exploitation action given WHM's full DNS management capability.
Forensic Artifacts	/var/log/cpanel-login.log and /var/log/whm-login.log — primary artifact for authentication bypass detection; successful session grants without preceding credential validation steps indicate bypass exploitation rather than legitimate login. | /var/cpanel/accounting.log — records all WHM-level administrative actions (createacct, modifyacct, setpwd, suspendacct) with source IP and timestamp; unauthorized account creation or privilege changes during the exposure window are a direct indicator of post-exploitation activity. | /home/*/authorized_keys and /root/.ssh/authorized_keys — SSH public keys injected by an attacker post-bypass grant persistent access independent of cPanel credentials; compare file modification timestamps against the exposure window and audit for unrecognized key fingerprints. | /home/*/public_html/ web shell artifacts — an attacker with WHM administrative access can deploy web shells to any hosted site; search with `find /home/*/public_html -name '*.php' -newer /tmp/exposure_start -exec grep -l 'eval(base64_decode' {} \;` to detect common obfuscated web shell patterns dropped during the exploitation window. | /var/named/ DNS zone files — WHM provides full DNS management, making DNS record modification (A record hijacking, MX record tampering for email interception) a high-probability attacker action; audit zone file modification timestamps and compare current records against last-known-good DNS snapshots or registrar records.

Per-Action IR Details

Step 1: Containment — immediately restrict inbound access to ports 2083 and 2087 at the firewall or network perimeter for all internet-facing cPanel/WHM servers; allow access only from known administrative IP ranges as a compensating control while patching proceeds.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On Linux-based cPanel servers, immediately apply iptables rules: `iptables -I INPUT -p tcp --dport 2083 -j DROP` and `iptables -I INPUT -p tcp --dport 2087 -j DROP`, then re-allow only trusted admin CIDRs: `iptables -I INPUT -s -p tcp --dport 2083 -j ACCEPT`. Persist rules with `iptables-save > /etc/sysconfig/iptables`. If cPanel's built-in ConfigServer Firewall (CSF) is installed, use `csf -d ` for blocking and update `/etc/csf/csf.allow` for trusted ranges. Verify rule order with `iptables -L INPUT -n --line-numbers`.

Evidence: Before blocking, capture current connection state: run `ss -tnp | grep -E '2083|2087'` and `netstat -anp | grep -E '2083|2087'` to document any active sessions on the cPanel/WHM ports. Export `/var/log/cpanel-login.log` and `/var/log/whm-login.log` (or equivalent cPanel authentication log paths) to preserve pre-containment access records. Also snapshot `last` and `lastb` output to capture recent successful and failed SSH and panel login history before any log rotation occurs.

Step 2: Detection — audit current cPanel/WHM version across all managed servers; review authentication logs on ports 2083 and 2087 for anomalous access attempts, successful logins from unrecognized IPs, or login events that lack preceding authentication challenge entries; look for unexpected account creation or

privilege changes in WHM audit logs.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Run `cat /usr/local/cpanel/version` on each server to confirm installed cPanel version and compare against patched release list. Parse cPanel authentication logs with: `grep -E 'PASS|SUCCESS' /var/log/cpanel-login.log | awk '{print $1, $2, $NF}' | sort | uniq -c | sort -rn` to surface high-frequency or unusual source IPs. For authentication bypass detection, specifically hunt for successful login events with no corresponding authentication challenge or MFA step by filtering `/var/log/cpanel-login.log` for entries where a session token was issued without a password hash validation record immediately preceding it. Review WHM audit log at `/var/cpanel/logs/archive/` and `/usr/local/cpanel/logs/` for `createacct`, `modifyacct`, or `setpwd` actions from unexpected users or IPs.

Evidence: Preserve `/var/log/cpanel-login.log`, `/var/log/whm-login.log`, `/usr/local/cpanel/logs/access_log`, and `/usr/local/cpanel/logs/error_log` before any log rotation. Capture WHM audit trail from `/var/cpanel/accounting.log` which records WHM-level account creation and modification actions with timestamps and source IPs. Export cPanel's `/var/cpanel/users/` directory listing to identify any accounts created during the exposure window. If cPanel's cPHulk brute force protection is enabled, export its database at `/var/cpanel/hulkd/` to correlate blocked vs. allowed authentication events — bypass exploitation would appear as successful logins without corresponding hulkd challenge records.

Step 3: Eradication — apply cPanel emergency patches immediately; target versions are 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 active branch; update via WHM >> cPanel >> Update Preferences or the command-line updater (/usr/local/cpanel/scripts/upcp).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run `/usr/local/cpanel/scripts/upcp --force` as root to force an immediate update to the latest patched branch version. For multi-server environments without a centralized patch management tool, script this across hosts using: `for host in ; do ssh root@$host '/usr/local/cpanel/scripts/upcp --force'; done`. After patching, confirm remediation with `cat /usr/local/cpanel/version` and validate the authentication module specifically by running `/usr/local/cpanel/scripts/check_cpanel_rpms --fix` to verify binary integrity of the authentication components. If the server is managed by a hosting provider (e.g., Namecheap), open an emergency escalation ticket referencing this authentication bypass and request immediate confirmation of patched version deployment.

Evidence: Before applying the patch, take a filesystem snapshot or at minimum capture: `rpm -qa | grep cpanel` to document all installed cPanel RPMs, `md5sum /usr/local/cpanel/Cpanel/Security/Authn/*.pm` to fingerprint authentication module files pre-patch for comparison post-patch, and a full copy of `/var/cpanel/users/` to baseline account state. If compromise is suspected, also collect running process list (`ps auxf`), active network connections (`ss -tnp`), and crontab entries for all cPanel-managed accounts (`for user in $(ls /var/cpanel/users/); do crontab -l -u $user 2>/dev/null; done`) before patching overwrites attacker persistence mechanisms.

Step 4: Recovery — after patching, verify installed version against the patched release list; re-enable port access only after version confirmation; audit all WHM and cPanel accounts for unauthorized changes, new accounts, modified SSH keys, altered DNS records, or added email forwarders that may indicate exploitation during the exposure window.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Verify patch success: `cat /usr/local/cpanel/version` must match a patched release. Audit for unauthorized accounts: `diff <(sort /var/cpanel/users_baseline.txt) <(ls /var/cpanel/users/ | sort)` — if no baseline exists, cross-reference `/var/cpanel/accounting.log` for `createacct` entries during the exposure window. Check for modified SSH authorized_keys across all hosted accounts: `find /home/*/. ssh/authorized_keys -newer /tmp/patch_timestamp -exec ls -la {} \; -exec cat {} \;`. Audit DNS zone modifications via `/var/named/` file timestamps or cPanel's DNS clustering logs. Review email forwarders by parsing `/etc/valiases/` for changes post-exposure using `find /etc/valiases/ -newer /tmp/patch_timestamp`. Re-enable ports 2083/2087 only after all checks pass: `iptables -D INPUT -p tcp --dport 2083 -j DROP`.

Evidence: Capture the full post-patch account state: export `/var/cpanel/users/` contents, all `authorized_keys` files under `/home/*/`, DNS zone files from `/var/named/`, and email forwarder configs from `/etc/valiases/`. Collect cPanel's FTP account list and database user grants for each hosted account to detect data exfiltration staging. Check `/var/log/secure` and `/var/log/auth.log` for post-exploitation SSH logins using keys that may have been injected via the bypass. Preserve these artifacts with timestamps before restoring normal operations, as they constitute the evidence record for any subsequent breach notification assessment.

Step 5: Post-Incident — evaluate whether cPanel administrative interfaces should ever be internet-facing without VPN or IP allowlisting; implement continuous version monitoring for cPanel/WHM to reduce time-to-patch on future emergency advisories; review hosting provider SLAs and patch notification channels to ensure emergency advisories reach the patching team within hours, not days.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Implement a daily cron job to alert on cPanel version drift: `echo '0 6 * * * root VER=$(cat /usr/local/cpanel/version); curl -s https://httpupdate.cpanel.net/cpanelsync/STABLE/version | grep -q "$VER" || echo "cPanel version $VER may be outdated" | mail -s "cPanel Version Alert" security@yourdomain.com' >> /etc/cron.d/cpanel-version-check`. Subscribe to cPanel security advisories via the official cPanel Security mailing list and CISA KEV feed (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) to catch emergency advisories without relying solely on hosting provider notification. For VPN-less environments, enforce cPanel/WHM access exclusively via SSH tunnel: document procedure `ssh -L 2087:localhost:2087 user@server` and make it the standard admin workflow, eliminating direct internet exposure of ports 2083/2087 permanently.

Evidence: Compile a full incident timeline documenting: first exposure date (based on cPanel version install timestamp from `rpm -qi cpanel`), first confirmed exploitation attempt (from cpanel-login.log analysis), containment time (firewall rule application timestamp), and patch completion time. This timeline is required for breach notification threshold assessment if PII or payment data was hosted on affected servers. Archive all log exports, account diffs, and forensic captures from Steps 1-4 per your retention policy (NIST AU-11 (Audit Record Retention)) with a minimum 12-month retention for potential regulatory review.

Detection Guidance

Query server authentication logs on ports 2083 and 2087 for successful session establishment events that lack a corresponding valid credential submission. Log file locations vary by hosting provider and cPanel configuration; typical paths include /usr/local/cpanel/logs/access_log and /var/log/cpanel/login_log. If you use a managed hosting provider (Namecheap, InMotion Hosting, etc.), request access log exports from their support team. In cPanel access logs, look for HTTP 200 responses to /login/?login_only=1 or /json-api/cpanel endpoints from IPs not in your administrative allowlist. In WHM, review Security Advisor logs and the Event Manager audit

trail for account modifications, root-level session creation, or API token generation not initiated by known administrators. Flag any login timestamp that does not correspond to a known maintenance window. No public IOC signatures (hashes, domains, IPs) have been released as of this writing. Recommend monitoring CISA KEV (cisa.gov/known-exploited-vulnerabilities) for 24-hour inclusion given active exploitation reports.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1190** — Exploit Public-Facing Application
- **T1556** — Modify Authentication Process
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **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
T1133	External Remote Services	Persistence
T1190	Exploit Public-Facing Application	Initial-Access
T1556	Modify Authentication Process	Credential-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/critical-cpanel-authentication.html	T3
cPanel Critical Authentication Bypass Actively Exploited - Hadrian.io	https://hadrian.io/blog/cpanel-critical-authentication-bypass-activ...	T3
cPanel WHM Critical Auth Bypass Fixed — Patch Now	https://www.thecybersignal.com/cpanel-whm-emergency-patch-critical-...	T3
cPanel & WHM Security Vulnerability – Temporary Access Restrictions	https://www.inmotionhosting.com/support/news/cpanel-whm-security-vu...	T3
cPanel Warns of Critical Authentication Flaw - Emergency Patch ...	https://cybersecuritynews.com/cpanel-authentication-flaw/	T3

Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-29 18:49 UTC by TJS Security Command Center