cPanel & WHM – Authentication Bypass Vulnerability Actively Exploited

TL;DR

There is an authentication bypass vulnerability in cPanel & WHM (CVE-2026-41940, CVSS 9.8).The flaw affects all supported versions and has already been exploited in the wild.

Attackers can bypass authentication controls and gain root-level access to hosting servers. Given that cPanel runs tens of millions of domains globally, this issue has wide impact and could lead to full server compromise, website takeovers, and data exposure if not patched immediately.

Overview

There is a vulnerability in cPanel & WHM (CVE-2026-41940, CVSS 9.8) caused by improper handling of session data and input sanitization. Attackers can use CRLF injection to tamper with session files and bypass authentication, which leads to root access.

Affected Products

- cPanel & WHM (all versions after 11.40 prior to patched releases)

cPanel & WHM is one of the most widely used web hosting control panels in the world, powering over 70 million domains across shared hosting environments, enterprise infrastructure, and managed service providers. This means a large portion of internet-facing infrastructure could be exposed if systems remain unpatched.

Exploitation has already been observed in the wild as a zero-day. CVE-2026-41940 targets the management plane of hosting servers, which controls user accounts, domains, email services, and server-level configurations. Once accessed, attackers essentially hold the keys to the entire environment.

Once exploited, the attacker controls the server. They can access data, change content, and use the system for their own activity. If that server connects to other systems, the issue can spread beyond a single host. If you have cPanel in your environment and it isn't patched, the server is exposed. Patch immediately.

Aspire Protects

- **Patch** – Update immediately. See the cPanel security advisory for patched versions and instructions on how to update via the cPanel update system.
- Run cPanel update:
  - `/scripts/upcp --force`
- Restart services after patching:
  - `/scripts/restartsrv_cpsrvd --hard`
- If patching is not immediately possible:
  - Block ports 2083, 2087, 2095, 2096 at the firewall
  - Disable cPanel service access temporarily
- Review session files for indicators of compromise
- Reset credentials for root and all privileged users if compromise is suspected

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit a vulnerable cPanel service exposed to the internet to bypass authentication and gain access.

Defense Evasion

- Impair Defenses [T1562] – The attacker may manipulate session handling and authentication logic to bypass security controls.

Persistence

- Valid Accounts [T1078] – The attacker may create or modify accounts after gaining root access to maintain long-term control of the system.

Host-Based IoCs (cPanel Session File Artifacts)

Behavioral

- Multiple failed login attempts followed by sudden authenticated session behavior
- Requests missing or manipulating `cp_security_token`
- Repeated `token_denied` increments in session files
- Authentication bypass without valid credentials

Log-Based Indicators

- cPanel access logs:
  - `/usr/local/cpanel/logs/access_log`

- Look for:
  - Requests to WHM endpoints without proper auth tokens
  - Suspicious use of ports:
    - 2083 (cPanel SSL)
    - 2087 (WHM SSL)
  - HTTP requests with malformed headers or unusual authentication patterns

File Integrity / Anomalies

- Session files containing malformed lines (not key=value format)
- Evidence of newline/CRLF injection artifacts inside session data

Targeted Industries

This vulnerability impacts any organization using cPanel-hosted infrastructure.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Security: CVE-2026-41940 - cPanel & WHM / WP2 Security Update 04/28/2026 – cPanel

CVE-2026-41940 | Tenable®

GitHub - XsanFlip/poc-cpanel-cve-2026-41940 · GitHub