NATIONAL CSIRT-CY

CVE-2026-41940
A Critical Authentication Bypass in cPanel

29 April 2026

[Cyber Threat Intelligence]

EXECUTIVE SUMMARY:

The Digital Security Authority (DSA) has observed a critical authentication bypass vulnerability in cPanel & WHM, including DNSOnly, and WP Squared. The issue affects cPanel software versions after 11.40 and can allow an unauthenticated remote attacker to gain unauthorized access to exposed hosting control panels. cPanel released patched versions and published official remediation and detection guidance.

TECHNICAL DETAILS:

Session-file manipulation through CRLF injection in HTTP Basic auth handling.

cPanel and WHM serve as the central authentication and administrative layer for shared hosting infrastructure. In properly segmented environments, the cpsrvd ports (2082/2083 (cPanel), 2086/2087 (WHM), and 2095/2096 (Webmail)) are not directly exposed to the internet. All three port pairs run the same cpsrvd binary against the same vulnerable session-handling code, so any of them is exploitable if reachable. Exposure frequently occurs through management convenience, temporary configurations, hybrid hosting scenarios, or firewall misconfigurations. Since authentication is bypassed entirely, exploitation depends only on network reachability.

Vulnerability Details

- **CVE ID:** CVE-2026-41940
- **CWE:** CWE-306 – Missing Authentication for Critical Function
  CWE-93 – Improper Neutralization of CRLF Sequences in HTTP Headers (per cPanel's advisory
  CWE-117 – Improper Output Neutralization for Logs/Files is arguably a closer fit, since the CRLF lands in an on-disk session file rather than a response header)
- **CVSS v4.0 Score:** **9.8 (Critical)**
- **Actively Exploited:** Yes
- **Impact:** Unauthenticated root administrative access to WHM, enabling control-plane manipulation and server-wide compromise.

Exploitation Status

- Product: cPanel/WHM
- Affected Versions: cPanel 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
- Fix: Upgrade to vendor-specified fixed releases; no workaround exists

RECOMMENDATIONS:

Organizations should treat cPanel/WHM as critical infrastructure. Response posture should prioritise patching, artifact preservation, and compromise assessment.

Immediate Actions

- Inventory all cPanel/WHM instances.

- Identify which instances were internet-exposed during the disclosure window (April 28–29, 2026).
- Upgrade to fixed releases:
    - 11.110.x → 11.110.0.97 or later
    - 11.118.x → 11.118.0.63 or later
    - 11.126.x → 11.126.0.54 or later
    - 11.132.x → 11.132.0.29 or later
    - 11.134.x → 11.134.0.20 or later
    - 11.136.x → 11.136.0.5 or later
- Verify the patch via /usr/local/cpanel/cpanel -V.
- If using a hosting provider, verify patch status with the provider directly.

Please ensure to distribute this information among your subsidiaries and partners and provide us with any pertinent information or findings you may have (such as Indicators of Compromise, Tactics, Techniques, and Procedures, etc.).

The Digital Security Authority (DSA) extends its appreciation for the continued collaboration.

REFERENCES:

1. https://docs.cpanel.net/release-notes/release-notes
2. https://docs.wpsquared.com/changelogs/versions/changelog/#13617
3. https://support.cpanel.net/hc/en-us/articles/40073787579671-cPanel-WHM-Security-Update-04-28-2026
4. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-41940
5. https://www.namecheap.com/status-updates/ongoing-critical-security-vulnerability-in-cpanel-april-28-2026
6. https://www.vulncheck.com/advisories/cpanel-and-whm-authentication-bypass-via-login-flow
7. https://github.com/watchtowrlabs/watchTowr-vs-cPanel-WHM-AuthBypass-to-RCE.py

DISCLAIMER:

The information presented in this report is based on available data up to the 29th of April 2026.

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.