



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Thursday, May 07, 2026

CSIC-ADVISORY-202605-A-002

Critical Function Vulnerability impacting WebPros cPanel, WebHost Manager, and WordPress Squared

Patch Available

Remote Authentication Bypass

Proof-of-Concept Available

Active Exploitation

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical function vulnerability impacting WebPros cPanel, WebHost Manager (WHM), and WordPress Squared (WP2). CVE-2026-41940 carries a CVSS 3.1 score of 9.8.¹ It is an authentication bypass caused by a Carriage Return Line Feed (CRLF) injection in the login and session loading processes of cPanel and WHM.

Successful exploitation allows unauthenticated remote attackers to bypass authentication to gain unauthorized administrative access to the targeted system. Additionally, it grants the attacker control over the cPanel host system, its configurations and databases, and the websites it manages.

A proof-of-concept and technical analysis for CVE-2026-41940 has been published, and there is confirmation of active exploitation in the wild.²

For additional technical vulnerability details and remediation instructions within the vendor's security advisory, please use these links:

Advisory: [Security: CVE-2026-41940 - cPanel & WHM / WP2 Security Update 04/28/2026 – cPanel](#)

Proof-of-Concept: <https://github.com/watchtowrlabs/watchTower-vs-cPanel-WHM-AuthBypass-to-RCE.py/blob/main/watchTower-vs-cPanel-WHM-AuthBypass-to-RCE.py>

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Product and Version:

Product	Version
cPanel and WebHost Manager	11.110.0 11.118.0 11.126.0 11.132.0 11.134.0 11.136.0
WordPress Squared	11.136.1

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References

¹ NVD; "CVE-2026-41940 Detail"; <https://nvd.nist.gov/vuln/detail/CVE-2026-41940>; accessed 04 May 2026

² Rapid7; "CVE-2026-41940: cPanel & WHM Authentication Bypass"; <https://www.rapid7.com/blog/post/etr-cve-2026-41940-cpanel-whm-authentication-bypass/>; accessed 04 May 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR