An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2609100238

NCSC Advisory

Critical Vulnerability in WebPros: cPanel/WHM
CVE-2026-67401

10th, September 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-67401

Published: 2026-09-09

Vendor: WebPros

Product: cPanel/WHM

CVSS Score[1]: 9.9

Products Affected

Product	Version
cPanel/WHM	0 < 11.134.0.55
cPanel/WHM	0 < 11.136.0.39
cPanel/WHM	0 < 11.138.0.4
cPanel/WHM	0 < 11.138.1.9
cPanel/WHM	0 < 11.110.0.143

Impact

A vulnerability in cPanel/WHM allows a mail-enabled account to achieve remote code execution as root through SQLi in EmailTrack component. Successful exploitation leads to code execution as the root user, giving an attacker full control of the server.

Common Weakness Enumeration (CWE)[2]: CWE-89: SQL Injection

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from WebPros.

- https://nvd.nist.gov/vuln/detail/CVE-2026-67401
- https://www.cve.org/CVERecord?id=CVE-2026-67401
- https://support.cpanel.net/hc/en-us/articles/43187903921559-Security-CVE-2026-67401-SQL-Injection-Vulnerability-in-cPanel-s-EmailTrack-Functionality-September-8-2026