Alert Bulletin

Bulletin N.: 81
Publication Date: 05/08/2026
Subject: Alert 2026-81 Critical vulnerability in cPanel & WHM SQL execution
Traffic Light Protocol (TLP): White

Affected product(s):

• cPanel & WHM – all supported versions prior to the fix builds
• WP Squared – all versions prior to 138.1.6

Description

A critical vulnerability has been disclosed in cPanel & WHM (CVSSv4.0: 9.4) that allows an authenticated hosting customer to execute arbitrary SQL with database root privileges, with possible impact at the operating system level. The same release fixes two additional high-severity vulnerabilities: HTTP request smuggling in cpsrvd and privilege escalation in Exim. It is recommended to immediately upgrade to the fixed builds or, as a temporary mitigation, revoke the MySQL feature from cPanel users from WHM.

cPanel & WHM is the most widely used web hosting management platform in the world, used by hosting providers, Linux server administrators, and companies to manage websites, databases, mail, and server configurations from a centralized interface. On August 4, 2026, cPanel published a targeted security release that fixes three vulnerabilities, including CVE 2026 58048 (CVSS 4.0: 9.4 – Critical), an SQL injection flaw that allows an authenticated hosting customer to execute SQL commands with database root privileges, crossing the privilege boundary between their account and the administrative identity of the server. CISA rated the technical impact as “total”, indicating that the compromise may extend to the operating system level depending on the environment configuration.

The reported vulnerabilities are listed below:

- CVE 2026 58048 – SQL Injection / Database Root Privilege Escalation (CVSS 4.0: 9.4 – Critical)
  The flaw resides in the database rename process in cPanel (CWE 89). When renaming a database, the SQL mode is not preserved correctly, causing SQL statements to be executed in the root context of the database server instead of the restricted context of the account user. An authenticated hosting customer can leverage this behavior to execute arbitrary SQL with full administrative privileges on the database engine, and potentially escalate the compromise to the operating system level.

- CVE 2026 58047 – HTTP Request Smuggling in cpsrvd (High)
  An HTTP request smuggling flaw in the cPanel cpsrvd daemon allows a remote unauthenticated attacker to abuse differences in HTTP request parsing to intercept or manipulate traffic, with risk of credential or session leakage from other users on the server.
- GCVE 25 2026 07 45 3 – Exim Privilege Escalation via .forward (High)
  A vulnerability in the Exim integration with cPanel allows a local user's .forward file to trigger an unsafe string expansion, which can be leveraged to execute commands with elevated privileges. This flaw is related to GCVE 25 2026 07 45 1, a local directory traversal vulnerability in Exim likewise usable for privilege escalation.

Mitigation

For CVE 2026 58048, if immediate upgrade is not possible, administrators can apply the following temporary mitigation:
• Revoke the MySQL feature from all cPanel users from the WHM panel until the patch is applied.
Note: This mitigation applies only to CVE 2026 58048. For CVE 2026 58047 and the Exim vulnerabilities there is no temporary mitigation; the only solution is to upgrade.

Solution

Upgrade to the patched builds indicated in the following table.
The upgrade can be performed from WHM □cPanel □Upgrade to Latest Version or by running the following command as root via SSH:

/usr/local/cpanel/scripts/upcp –force

Product and installed version Fixed version Upgrade information
cPanel & WHM branch 11.110.x 11.110.0.137 https://cpanel.net/security/advisories/
cPanel & WHM branch 11.118.x 11.118.0.71 https://cpanel.net/security/advisories/
cPanel & WHM branch 11.126.x 11.126.0.78 https://cpanel.net/security/advisories/
cPanel & WHM branch 11.134.x 11.134.0.48 https://cpanel.net/security/advisories/
cPanel & WHM branch 11.136.x 11.136.0.32 https://cpanel.net/security/advisories/
WP Squared 138.1.6 https://cpanel.net/security/advisories/

Additional information:

• The Hacker News – New cPanel Critical Flaw Could Let Hosting Customers Run SQL as Database Root
https://thehackernews.com/2026/08/new-cpanel-critical-flaw-could-let.html
• cPanel Security Advisories
https://cpanel.net/security/advisories/
• NVD – CVE 2026 58048
https://nvd.nist.gov/vuln/detail/CVE-2026-58048
• NVD – CVE 2026 58047

https://nvd.nist.gov/vuln/detail/CVE-2026-58047

• CISA – Known Exploited Vulnerabilities Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog