Boletín de alerta

Boletín Nro.: 81
Fecha de publicación: 05/08/2026
Tema: Alerta 2026-81 Vulnerabilidad critica en cPanel & WHM de ejecucion SQL
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

• cPanel & WHM – todas las versiones soportadas anteriores a los builds de corrección
• WP Squared – todas las versiones anteriores a 138.1.6

Descripción

Se ha publicado una vulnerabilidad crítica en cPanel & WHM (CVSSv4.0: 9.4) que permite a un cliente de hosting autenticado ejecutar SQL arbitrario con privilegios de root de base de datos, con posible impacto a nivel de sistema operativo. El mismo release corrige dos vulnerabilidades adicionales de severidad alta: HTTP request smuggling en cpsrvd y escalada de privilegios en Exim. Se recomienda actualizar de forma inmediata a los builds corregidos o, como mitigación temporal, revocar el feature de MySQL a los usuarios de cPanel desde WHM.

cPanel & WHM es la plataforma de administración de hosting web más utilizada en el mundo, empleada por proveedores de hosting, administradores de servidores Linux y empresas para gestionar sitios web, bases de datos, correos y configuraciones de servidor desde una interfaz centralizada. El 4 de agosto de 2026, cPanel publicó una targeted security release que corrige tres vulnerabilidades, incluyendo CVE 2026 58048 (CVSS 4.0: 9.4 – Crítico), una falla de inyección SQL que permite a un cliente de hosting autenticado ejecutar comandos SQL con privilegios de root de base de datos, cruzando el límite de privilegios entre su cuenta y la identidad administrativa del servidor. CISA calificó el impacto técnico como «total», indicando que el compromiso puede extenderse al nivel del sistema operativo dependiendo de la configuración del entorno.

A continuación se listan las vulnerabilidades reportadas:

- CVE 2026 58048 – SQL Injection / Database Root Privilege Escalation (CVSS 4.0: 9.4 – Crítico)
  La falla reside en el proceso de renombrado de bases de datos en cPanel (CWE 89). Al renombrar una base de datos, el SQL mode no se preserva correctamente, lo que provoca que las instrucciones SQL se ejecuten en el contexto root del servidor de base de datos en lugar del contexto restringido del usuario de la cuenta. Un cliente de hosting autenticado puede aprovechar este comportamiento

para ejecutar SQL arbitrario con privilegios administrativos completos sobre el motor de base de datos, y potencialmente escalar el compromiso al nivel del sistema operativo.

- CVE 2026 58047 – HTTP Request Smuggling en cpsrvd (High)
  Una falla de HTTP request smuggling en el daemon cpsrvd de cPanel permite a un atacante remoto no autenticado abusar de diferencias en el parseo de peticiones HTTP para interceptar o manipular tráfico, con riesgo de filtración de credenciales o sesiones de otros usuarios del servidor.
- GCVE 25 2026 07 45 3 – Exim Privilege Escalation vía .forward (High)
  Una vulnerabilidad en la integración de Exim con cPanel permite que el archivo .forward de un usuario local desencadene una expansión de cadenas no segura, lo que puede ser aprovechado para ejecutar comandos con privilegios elevados. Esta falla está relacionada con GCVE 25 2026 07 45 1, una vulnerabilidad de directory traversal local en Exim igualmente utilizable para escalada de privilegios.

Mitigación

Para CVE 2026 58048, si la actualización inmediata no es posible, los administradores pueden aplicar la siguiente mitigación temporal:
• Revocar el feature de MySQL a todos los usuarios de cPanel desde el panel de WHM hasta que el parche sea aplicado.
Nota: Esta mitigación aplica únicamente a CVE 2026 58048. Para CVE 2026 58047 y las vulnerabilidades de Exim no existe mitigación temporal; la única solución es actualizar.

Solución

Actualizar a los builds parcheados que se indican en la siguiente tabla.
La actualización puede realizarse desde WHM cPanel Upgrade to Latest Version o ejecutando el siguiente comando como root vía SSH:

/usr/local/cpanel/scripts/upcp –force

Producto y versión instalada Versión corregida Información de actualización
cPanel & WHM rama 11.110.x 11.110.0.137 https://cpanel.net/security/advisories/
cPanel & WHM rama 11.118.x 11.118.0.71 https://cpanel.net/security/advisories/
cPanel & WHM rama 11.126.x 11.126.0.78 https://cpanel.net/security/advisories/
cPanel & WHM rama 11.134.x 11.134.0.48 https://cpanel.net/security/advisories/
cPanel & WHM rama 11.136.x 11.136.0.32 https://cpanel.net/security/advisories/
WP Squared 138.1.6 https://cpanel.net/security/advisories/

Información adicional:

• 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