Boletín de alerta

Boletín Nro.: 94
Fecha de publicación: 28/08/2026
Tema: Alerta 2026-94 Vulnerabilidad crítica en cPanel /WHM
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

cPanel/WHM: todas las versiones soportadas anteriores a:

- 11.110.0.141
- 11.134.0.53
- 11.136.0.37
- 11.138.0.2

WP² (WP Squared):

- versiones anteriores a 11.138.1.7

Descripción

El 27 de agosto de 2026, cPanel publicó un aviso de seguridad sobre la vulnerabilidad **CVE-2026-65643**, una falla crítica en la funcionalidad de dominios estacionados (parked domains) y dominios adicionales (addon domains) de cPanel/WHM, plataforma de administración ampliamente utilizada en servicios de alojamiento web. El fabricante no ha publicado una puntuación CVSS; sin embargo, clasifica el problema como crítico debido al impacto de una explotación exitosa.

La falla permite que un titular de cuenta cPanel ya autenticado, con permisos para añadir dominios estacionados o adicionales, cree archivos arbitrarios en el servidor. Esta capacidad puede encadenarse para conseguir ejecución de código con privilegios de root, comprometiendo por completo el sistema operativo subyacente.

Como consecuencia, un atacante podría obtener control total del servidor y acceder o manipular todas las cuentas de hosting, sitios web, aplicaciones y bases de datos alojadas. El vector requiere autenticación

previa, pero representa un riesgo especialmente alto en ambientes de hosting compartido o de revendedores, donde una cuenta de bajo privilegio podría convertirse en el punto de entrada para afectar a múltiples clientes.

Hasta el 28 de agosto de 2026, el fabricante no ha informado explotación activa, publicado un PoC, ni detallado públicamente el componente exacto o mecanismo interno que permite la escritura arbitraria. Tampoco se ha publicado un registro CVE con métricas CVSS oficiales.

Solución:

Se recomienda actualizar inmediatamente cPanel/WHM a la versión corregida correspondiente a la rama instalada. El aviso y las versiones corregidas del fabricante están disponibles en el **parche oficial de cPanel.**

La actualización puede ejecutarse desde WHM, en Home > cPanel > Upgrade to Latest Version, o mediante SSH con privilegios de root usando:

/usr/local/cpanel/scripts/upcp –force

Los sistemas que ejecuten versiones fuera de soporte deben migrar a una rama soportada para recibir la corrección. Como medida temporal, si no es posible actualizar de inmediato, conviene restringir o deshabilitar para cuentas no administrativas la capacidad de añadir dominios estacionados y dominios adicionales, reduciendo la superficie de ataque hasta completar la actualización.

Información adicional:

- **https://support.cpanel.net/hc/en-us/articles/42959571221527-Security-CVE-2026-65643-Vulnerability-in-cPanel-s-Domain-Parking-Functionality-August-27-2026**
- **https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-cpanel-y-whm-permite-escalada-a-root/**
- **https://thehackernews.com/2026/08/critical-cpanel-flaw-could-let-one.html**