Boletín de alerta

Boletín Nro.:
Fecha de publicación: 30/04/2026
Tema: Alerta 2026-44 Vulnerabilidad cPanel/WHM
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- cPanel & WHM: versiones 11.110.0.97, 11.118.0.63, 11.126.0.54, 11.132.0.29, 11.136.0.5 y 11.134.0.20

Descripción

Se ha identificado la vulnerabilidad CVE-2026-41940, catalogada como crítica, que afecta a cPanel, que podría permitir a un atacante comprometer la seguridad de sistemas afectados dependiendo de su configuración y nivel de exposición.

WHM y cPanel, son paneles de control de alojamiento web basados en Linux para la administración de servidores y sitios web. Mientras que WHM proporciona control a nivel de servidor, cPanel ofrece acceso de administrador al backend del sitio web, el correo web y las bases de datos.

La vulnerabilidad está relacionada con un manejo inadecuado de validaciones o controles internos, lo que podría ser aprovechado para ejecutar acciones no autorizadas dentro del entorno objetivo.

Una explotación exitosa podría permitir:

- Ejecución remota de código (RCE)
- Acceso no autorizado a recursos del sistema
- Escalamiento de privilegios
- Manipulación de procesos o servicios críticos

Solución y mitigaciones:

Se recomienda a las organizaciones implementar de manera inmediata las siguientes acciones:

- Los usuarios que utilicen software no compatible deben migrar inmediatamente a un entorno de servidor compatible, ya que las versiones antiguas no recibirán parches de seguridad.
- Actualizar cPanel y WebHost Manager (WHM) a una versión parcheada de las indicadas anteriormente.

- Verificar con su proveedor de hosting si se esta usando cpanel, de ser así asegurarse que se actualice o tomado medidas compensatorias necesarias.
- Los administradores del servidor pueden forzar manualmente el proceso de actualización mediante la interfaz de línea de comandos, además de confirmar la versión instalada.
- Restringir el acceso a la red a las interfaces de cPanel/WHM (por ejemplo, mediante listas de direcciones IP permitidas en el firewall) hasta que se apliquen los parches.

Información adicional:

- https://www.bleepingcomputer.com/news/security/cpanel-whm-emergency-update-fixes-critical-auth-bypass-bug/?utm_source=dlvr.it&utm_medium=twitter
- https://labs.watchtowr.com/the-internet-is-falling-down-falling-down-falling-down-cpanel-whm-authentication-bypass-cve-2026-41940/
- https://hadrian.io/de/blog/cpanel-critical-authentication-bypass-actively-exploited