cPanel ha publicado actualizaciones de seguridad para corregir una vulnerabilidad que afecta distintos procesos de autenticación y que podría permitir a un atacante obtener acceso al software del panel de control.

El inconveniente impacta a todas las versiones actualmente compatibles, según una alerta emitida por cPanel el martes. La falla ya fue solucionada en las siguientes versiones:

- 11.110.0.97
- 11.118.0.63
- 11.126.0.54
- 11.132.0.29
- 11.136.0.5
- 11.134.0.20

«Si tu servidor no está ejecutando una versión compatible de cPanel que pueda recibir esta actualización, se recomienda encarecidamente trabajar en su actualización lo antes posible, ya que también podría verse afectado», señaló cPanel.

Aunque cPanel no proporcionó detalles técnicos sobre la vulnerabilidad, la empresa de hosting y registro de dominios Namecheap indicó que *«está relacionada con un exploit en el inicio de sesión de autenticación que podría permitir acceso no autorizado al panel de control»*.

Como medida preventiva, la compañía implementó una regla de firewall para bloquear el acceso a los puertos TCP 2083 y 2087, una acción que, según explicó, limitará temporalmente el acceso de los clientes a las interfaces de cPanel y WHM hasta que se aplique un parche completo.

«Nuestro equipo está monitoreando activamente la situación y aplicará el parche oficial en todos los servidores compatibles tan pronto como esté disponible», indicó Namecheap. *«El acceso a tus paneles de control será restablecido de inmediato una vez que el parche haya sido implementado con éxito»*.

Hasta el 29 de abril de 2026 a las 02:42 a.m. UTC, la corrección ya había sido aplicada en servidores Reseller, Stellar Business y otros, según el equipo de soporte de Namecheap.