cPanel, el popular administrador de alojamiento web, corrigió una vulnerabilidad de seguridad que pudo haber permitido a los hackers remotos con acceso a credenciales válidas, iniciar sesión omitiendo la autenticación de dos factores (2FA) en una cuenta.

La vulnerabilidad rastreada como SEC-575 y descubierta por investigadores de Digital Defense, ha sido solucionada por la compañía en las versiones 11.92.0.1, 11.90.0.17 y 11.86.0.32 del software.

cPanel y WHM (Web Host Manager) ofrecen un panel de control basado en Linux para que los usuarios manejen la administración de sitios web y servidores, incluidas las tareas como agregar subdominios y realizar el mantenimiento del panel de control y del sistema. Hasta ahora, se han lanzado más de 70 millones de dominios en servidores utilizando el paquete de software de cPanel.

Los investigadores de Digital Defense afirmaron que un ataque de este tipo podría lograrse en pocos minutos.

> *«La Política de Seguridad de cPanel de autenticación de dos factores no evitó que un atacante enviara repetidamente códigos de autenticación de dos factores. Esto permitió a un atacante eludir la verificación de autenticación de dos factores utilizando técnicas de fuerza bruta»,* dijo cPanel en un aviso.

La compañía ya abordó el problema agregando una verificación de límite de tasa a su servicio de protección de fuerza bruta cPHulk, lo que hace que una validación fallida del código 2FA se trate como un inicio de sesión fallido.

Esta no es la primera vez que la ausencia de una limitación de las tasas plantea un grave problema de seguridad.

En julio pasado, la aplicación de videoconferencia Zoom solucionó una laguna de seguridad que podría haber permitido a posibles atacantes descifrar el código de acceso numérico

utilizado para asegurar reuniones privadas en la plataforma y espiar a los participantes.