Cisco lanzó parches para contener una vulnerabilidad de seguridad crítica que afecta al controlador LAN inalámbrico (WLC), que podría ser abusada por un atacante remoto no autenticado para tomar el control de un sistema afectado.

Rastreada como CVE-2022-20695, la vulnerabilidad recibió una puntuación de 10 sobre 10 en gravedad, y permite que un atacante omita los controles de autenticación e inicie sesión en el dispositivo por medio de la interfaz de administración de WLC.

> *«Esta vulnerabilidad se debe a la implementación incorrecta del algoritmo de validación de contraseñas. Un atacante podría explotar esta vulnerabilidad iniciando sesión en un dispositivo afectado con credenciales manipuladas»,* dijo la compañía.

La explotación exitosa de la falla podría permitir que un atacante obtenga privilegios de administrador y lleve a cabo acciones maliciosas de una forma que permita tomar el control completo del sistema vulnerable.

La compañía enfatizó que el problema solo afecta a los siguientes productos si se ejecuta la versión 8.10.151.0 o la versión 8.10.162.0 del software WLC de Cisco y la compatibilidad con el radio de macfilter está configurada como Otro:

- Controlador inalámbrico 3504
- Controlador inalámbrico 5520
- Controlador inalámbrico 8540
- Movilidad Express
- Controlador inalámbrico virtual (vWLC)

Se recomienda a los usuarios que actualicen a la versión 8.10.171.0 para corregir la vulnerabilidad. Cisco Wireless LAN Controller versiones 8.9 y anteriores, así como 8.10.142.0 y anteriores, no son vulnerables.

Cisco brindó el crédito a un investigador no identificado en Bispok por informar sobre la

vulnerabilidad, afirmando que no hay evidencia de que CVE-2022-20695 esté siendo explotada activamente en la naturaleza.