El sistema de administración de dispositivos móviles (MDM) de FileWave, resultó vulnerable a dos fallas de seguridad críticas que podrían aprovecharse para realizar ataques remotos y tomar el control de una flota de dispositivos conectados a él.

> *«Las vulnerabilidades se pueden explotar remotamente y permiten a un atacante eludir los mecanismos de autenticación y obtener un control total sobre la plataforma MDM y sus dispositivos administrados»,* dijo Noam Moshe, investigador de seguridad de Claroty.

FileWave MDM es una solución de administración de dispositivos móviles multiplataforma que permite a los administradores de TI administrar y monitorear todos los dispositivos de una organización, incluyendo teléfonos móviles, tabletas, computadoras portátiles, estaciones de trabajo y televisores inteligentes.

La plataforma funciona como un canal para enviar software y actualizaciones obligatorios, cambiar la configuración del dispositivo e incluso borrar dispositivos remotamente, todo lo cual se entrega desde un servidor central.

Los dos problemas identificados por la compañía de tecnología operativa se relacionan con una omisión de autenticación (CVE-2022-34907) y el uso de una clave criptográfica codificada (CVE-2022-34906) que podría permitir a un atacante abusar de las funciones legítimas para exfiltrar datos confidenciales e instalar paquetes maliciosos.

Claroty dijo que descubrió más de 1,100 servidores FileWave vulnerables con acceso a Internet que pertenecen a sectores gubernamentales, educativos y de grandes empresas, cada uno con un *«número ilimitado de dispositivos administrados».*

Si las debilidades se explotan exitosamente, un adversario remoto podría obtener acceso privilegiado no autorizado a las instancias accesibles por Internet y apoderarse de los dispositivos administrados, otorgando carta blanca de acceso a todos los activos digitales en la red.

> *«Esto nos permite controlar todos los dispositivos administrados de los servidores, filtrar todos los datos confidenciales que tienen los dispositivos, incluidos nombres de usuario, direcciones de correo electrónico, direcciones IP, ubicación geográfica, etcétera, e instalar software malicioso en los dispositivos administrados»*, explicó Moshe.

Después de la divulgación responsable, los problemas se abordaron en la versión 14.7.2 lanzada el 14 de julio de 2022. Se insta a los usuarios de Filewave a aplicar la actualización lo antes posible para evitar ser víctimas de un ataque.

Los resultados subrayan una vez más la necesidad de proteger los dispositivos de gestión de terminales en la cadena de suministro de software. El año pasado, el grupo de ciberdelincuentes REvil abusó de una vulnerabilidad de día cero en la solución de administración de TI de Kaseya para implementar ransomware contra 1500 empresas de procesamiento.