La compañía de tecnología estadounidense, Kaseya, lanzó parches de seguridad para abordar dos vulnerabilidades de día cero, que afectan a su solución de continuidad y respaldo empresarial Unitrends, lo que podría resultar en una escalada de privilegios y ejecución remota de código autenticado.

Las dos vulnerabilidades son parte de 3 vulnerabilidades descubiertas e informadas por investigadores del Instituto Holandés de Divulgación de Vulnerabilidades (DIVD) el 3 de julio de 2021.

El proveedor de soluciones de gestión de infraestructura de TI abordó los problemas en la versión de software de servidor 10.5.5-2 lanzada el 12 de agosto, según DIVD. Una vulnerabilidad del lago del cliente aún no revelada en Kaseya Unitrends permanece sin parchear, pero la compañía publicó reglas de firewall que se pueden aplicar para filtrar el tráfico hacia y desde el cliente y mitigar cualquier riesgo asociado con la falla. Como precaución adicional, se recomienda no dejar los servidores accesibles a través de Internet.

Aunque los detalles relacionados con las vulnerabilidades son escasos, las deficiencias se refieren a una vulnerabilidad de ejecución remota de código autenticado, así como una falla de escalada de privilegios de usuario de solo lectura a administrador en servidores Unitrends, los cuales dependen de la posibilidad de que un atacante ya haya obtenido un punto de apoyo inicial en la red de un objetivo, lo que los hace más difíciles de explotar.

La divulgación de produce casi dos meses después de que la compañía sufriera un ataque de ransomware paralizante en su producto local VSA, lo que llevó al misterioso cierre del sindicato de delitos informáticos REvil en las siguientes semanas.

Desde entonces, Kaseya ha enviado arreglos para los días cero que fueron explotados para obtener acceso a los servidores en las instalaciones, y a fines del mes pasado, dijo que obtuvo un descifrador universal *«para remediar a los clientes afectados por el incidente».*