Los usuarios del software de transferencia de archivos administrado por Cleo han recibido advertencias para asegurarse de que sus instancias no estén accesibles desde internet, tras informes sobre la explotación masiva de una vulnerabilidad que afecta incluso a sistemas completamente actualizados.

La empresa de ciberseguridad Huntress reveló el 3 de diciembre de 2024 que detectó actividad maliciosa explotando esta falla de manera generalizada. La vulnerabilidad, presente en las aplicaciones LexiCom, VLTransfer y Harmony de Cleo, permite la ejecución remota de código sin necesidad de autenticación.

## Descripción de la vulnerabilidad

Identificada como CVE-2024-50623, la falla se debe a la posibilidad de cargar archivos sin restricciones, lo que facilita la ejecución de código arbitrario. Cleo, una compañía con sede en Illinois que cuenta con más de 4,200 clientes a nivel mundial, emitió un segundo aviso sobre otra vulnerabilidad, aún sin CVE asignado, que también podría permitir la ejecución remota de código mediante hosts malintencionados no autenticados.

## Impacto y actualizaciones

Según Huntress, los parches lanzados para CVE-2024-50623 no resuelven completamente el problema subyacente. Los productos afectados son los siguientes y se espera que reciban nuevas actualizaciones esta semana:

- Cleo Harmony (hasta la versión 5.8.0.23)
- Cleo VLTrader (hasta la versión 5.8.0.23)
- Cleo LexiCom (hasta la versión 5.8.0.23)

Los atacantes han explotado esta vulnerabilidad para insertar múltiples archivos maliciosos, incluyendo un archivo XML diseñado para ejecutar comandos PowerShell incrustados. Estos comandos descargan un archivo JAR (Java Archive) desde un servidor remoto.

La explotación se basa en que los archivos colocados en el subdirectorio «autorun» dentro de la carpeta de instalación son procesados automáticamente por el software vulnerable.

## Consecuencias de los ataques

Hasta ahora, al menos 10 organizaciones han tenido sus servidores Cleo comprometidos, con un aumento en los ataques registrado el 8 de diciembre de 2024, alrededor de las 7:00 a.m. UTC. Los primeros indicios de actividad maliciosa se remontan al 3 de diciembre de 2024. Las víctimas incluyen empresas de productos de consumo, logística, transporte y alimentación.

Para protegerse de esta amenaza, se insta a los usuarios a actualizar su software a la última versión disponible.

## Actores y tácticas involucrados

Grupos de ransomware como Cl0p (también conocido como Lace Tempest) han dirigido ataques contra herramientas de transferencia de archivos en el pasado, y esta actividad parece seguir un patrón similar. El investigador Kevin Beaumont (alias GossiTheDog) señaló que *«los operadores del grupo Termite (y posiblemente otros) están utilizando un exploit de día cero para las aplicaciones LexiCom, VLTransfer y Harmony de Cleo.»*

La empresa de ciberseguridad Rapid7 confirmó que se han explotado estas vulnerabilidades con éxito en entornos de clientes. Además, el grupo Termite ha asumido la autoría de un reciente ciberataque contra la empresa de cadenas de suministro Blue Yonder.

El equipo Symantec Threat Hunter de Broadcom indicó que Termite emplea una versión modificada del ransomware Babuk, el cual cifra archivos y les agrega la extensión .termite. Según Huntress, Blue Yonder tenía una instancia del software de Cleo expuesta a internet, lo que facilitó el ataque.

## Tendencias y especulaciones

Se especula que Termite podría ser una evolución del grupo Cl0p, ya que las actividades de Cl0p han disminuido mientras que las de Termite han aumentado. Aunque no hay pruebas definitivas, ambas organizaciones muestran similitudes en sus métodos operativos.