Las vulnerabilidades Zero-day en los instaladores de Windows para el software de monitoreo y administración remota de Atera podrían ser utilizadas como punto de partida para lanzar ataques de escalada de privilegios.

Las fallas, descubiertas por Mandiant el 28 de febrero de 2023, han sido asignadas los identificadores CVE-2023-26077 y CVE-2023-26078. Los problemas se han solucionado en las versiones 1.8.3.7 y 1.8.4.9 lanzadas por Atera el 17 de abril de 2023 y el 26 de junio de 2023, respectivamente.

> *«La capacidad de iniciar una operación desde un contexto NT AUTHORITY\SYSTEM puede presentar riesgos de seguridad potenciales si no se administra correctamente. Por ejemplo, las Acciones Personalizadas mal configuradas que se ejecutan como NT AUTHORITY\SYSTEM pueden ser explotadas por atacantes para ejecutar ataques locales de escalada de privilegios»,* dijo el investigador de seguridad Andrew Oliveau.

La explotación efectiva de estas debilidades podría allanar el camino para la ejecución de código arbitrario con privilegios elevados.

Ambas debilidades se localizan en la funcionalidad de reparación del instalador MSI, lo que podría crear una situación en la que las operaciones se desencadenan desde un contexto NT AUTHORITY\SYSTEM aunque sean iniciadas por un usuario estándar.

De acuerdo con una firma de inteligencia de amenazas propiedad de Google, Atera Agent es susceptible a un ataque local de escalada de privilegios que se puede explotar mediante la inyección DLL (CVE-2023-26077), lo que permitiría obtener un Símbolo del sistema como usuario NT AUTHORITY\SYSTEM.

Por otro lado, CVE-2023-26078 se refiere a la *«ejecución de comandos del sistema que activan el Host de Consola de Windows (conhost.exe) como un proceso secundario»*, lo que abre una *«ventana de comandos que, si se ejecuta con privilegios elevados, puede ser*

explotada por un atacante para realizar un ataque local de escalada de privilegios».

> *«Las Acciones Personalizadas mal configuradas pueden ser fácilmente identificables y explotables, lo que representa riesgos significativos para las organizaciones. Es esencial que los desarrolladores de software revisen cuidadosamente sus Acciones Personalizadas para impedir que los atacantes secuestren las operaciones NT AUTHORITY\SYSTEM desencadenadas por las reparaciones MSI»,* comentó Oliveau.

La divulgación se produce cuando Kaspersky arrojó más luz sobre una falla grave de escalada de privilegios ya corregida en Windows (CVE-2023-23397, puntuación CVSS: 9.8) que ha sido objeto de explotación activa en la naturaleza por actores de amenazas que utilizan una tarea de Outlook, un mensaje o un evento de calendario especialmente diseñados.

Si bien Microsoft reveló anteriormente que grupos estatales rusos habían utilizado la vulnerabilidad desde abril de 2022, la evidencia recopilada por el proveedor de antivirus ha revelado que se llevaron a cabo intentos reales de explotación por parte de un atacante desconocido que apuntaba a entidades gubernamentales e infraestructuras críticas en Jordania, Polonia, Rumania, Turquía y Ucrania un mes antes de la divulgación pública.