Los investigadores de ciberseguridad han detallado cuatro vulnerabilidades diferentes en un componente clave del servicio de programación de tareas de Windows, las cuales podrían ser explotadas por atacantes locales para lograr una escalada de privilegios y borrar registros, con el fin de ocultar evidencia de actividades maliciosas.

Las vulnerabilidades fueron descubiertas en un archivo binario llamado «schtasks.exe«, que permite a los administradores crear, eliminar, consultar, modificar, ejecutar y finalizar tareas programadas en computadoras locales o remotas.

Uno de los problemas identificados se refiere a una vulnerabilidad en el Control de Cuentas de Usuario (UAC) de Microsoft Windows, lo que permite a los atacantes evadir el aviso de UAC. Esto les posibilita ejecutar comandos con privilegios elevados (nivel SYSTEM) sin que el usuario lo apruebe. Según Ruben Enkaoua, investigador de seguridad en Cymulate, *«explotando esta vulnerabilidad, los atacantes pueden elevar sus privilegios y ejecutar cargas maliciosas con derechos de administrador, lo que lleva a accesos no autorizados, robo de datos o a un mayor compromiso del sistema».*

Este problema ocurre cuando un atacante crea una tarea programada usando Batch Logon (es decir, usando una contraseña) en lugar de un token interactivo, lo que hace que el servicio de programación de tareas otorgue al proceso ejecutado los máximos privilegios posibles.

Sin embargo, para que este ataque funcione, el atacante debe obtener la contraseña mediante otros métodos, como descifrar un hash NTLMv2 tras autenticarse en un servidor SMB, o explotar otras vulnerabilidades como CVE-2023-21726.

El resultado es que un usuario con pocos privilegios puede aprovechar el binario schtasks.exe para suplantar a miembros de grupos como administradores, operadores de copia de seguridad y usuarios de registro de rendimiento, utilizando una contraseña conocida para obtener los máximos privilegios posibles.

Además, el registro de una tarea programada mediante el uso de autenticación de inicio de

sesión por lotes con un archivo XML podría habilitar dos técnicas de evasión de defensa. Estas permitirían sobrescribir el registro de eventos de tareas, eliminando eficazmente las huellas de auditoría de actividades anteriores, así como desbordar los registros de seguridad.

Un ejemplo de esto sería registrar una tarea con un autor cuyo nombre, por ejemplo, tiene la letra «A» repetida 3,500 veces en el archivo XML. Esto provocaría la sobrescritura completa de la descripción del registro de tareas. Este comportamiento también podría extenderse para sobrescribir toda la base de datos de registros de seguridad en «C:\Windows\System32\winevt\logs\Security.evtx».

Enkaoua comentó sobre el interés del componente Programador de Tareas al decir: *«Es accesible para cualquiera que esté dispuesto a crear una tarea, iniciada por un servicio en ejecución de SYSTEM, manipulando privilegios, integridades de proceso y suplantaciones de usuarios»*. Añadió que *«la primera vulnerabilidad reportada no es solo un desvío de UAC, es mucho más que eso: es básicamente una manera de hacerse pasar por cualquier usuario con su contraseña de CLI y obtener los máximos privilegios posibles en la sesión de ejecución de tareas usando los indicadores /ru y /rp».*