Investigadores de seguridad cibernética revelaron este miércoles tres vulnerabilidades de seguridad graves, que afectan a los productos SolarWinds, la más grave de estas, podría haberse aprovechado para lograr la ejecución remota de código con privilegios elevados.

Dos vulnerabilidades (CVE-2021-25274 y CVE-2021-25275) se identificaron en la plataforma SolarWinds Orion, mientras que la tercera (CVE-2021-25276) se encontró en el servidor FTP Serv-U de la compañía para Windows, según informó la compañía de seguridad Trustwave.

Ninguna de las tres vulnerabilidades se aprovechó en el ataque anterior a la cadena de suministro dirigido a la plataforma Orion que salió a la luz en diciembre de 2020.

Los dos conjuntos de vulnerabilidades en Orion y Serv-U FTP se revelaron a SolarWinds el 30 de diciembre de 2020 y el 4 de enero de 2021, respectivamente, después de eso, la compañía resolvió los problemas el 22 de enero y el 25 de enero.

Se recomienda a los usuarios que instalen las últimas versiones de Orion Platform y Serv-U FTP (15.2.2 Hotfix 1) para mitigar los riesgos asociados con las vulnerabilidades. Trustwave dijo que su intención es lanzar un código de prueba de concepto (PoC) el 9 de febrero.

Control total de Orion

La principal de las vulnerabilidades descubiertas incluye el uso inapropiado de Microsoft Messaging Qeue (MSMQ), que es muy utilizado por SolarWinds Orion Collector Service, lo que permite que los usuarios no autenticados envíen mensajes a dichas colas por medio del puerto TCP 1801 y finalmente, obtener RCE al encadenarlo con otro problema de deserialización inseguro en el código que maneja los mensajes entrantes.

> *«Debido a que el código de procesamiento de mensajes se ejecuta como un servicio de Windows configurado para usar la cuenta LocalSystem, tenemos un control completo del sistema operativo subyacente»*, dijo Martin Rakhmanov, investigador de Trustwave.

El parche lanzado por SolarWinds (Orion Platform 2020.2.4) aborda el error con un paso de validación de firma digital que se realiza en los mensajes recibidos para garantizar que los mensajes sin firmar no se procesen más, pero Rakhmanov advirtió que el MSMQ aún no está autenticado y permite que cualquier pueda enviar mensajes a ella.

La segunda vulnerabilidad, también en la plataforma Orion, se refiere a la forma insegura en la que las credenciales de la base de datos backend (*SOLARWINDS_ORION*) se almacenan en un archivo de configuración, lo que resulta en un usuario local sin privilegios que toma el control total de la base de datos, roba información, o incluso agrega un nuevo usuario de nivel de administrador para utilizarlo dentro de los productos de SolarWinds Orion.

Finalmente, la vulnerabilidad en SolarWinds Serv-U FTP Server 15.2.1 para Windows, podría permitir que cualquier atacante que pueda iniciar sesión en el sistema local o mediante escritorio remoto suelte un archivo que define un nuevo usuario administrador con acceso completo a C:\unidad, que luego se puede aprovechar iniciando sesión como ese usuario a través de FTP y leer o reemplazar cualquier archivo en la unidad.

Esta noticia surge rápidamente luego de algunos informes de que supuestos hackers chinos explotaron una falla previamente indocumentada en el software de la compañía para ingresar al Centro Nacional de Finanzas, una agencia federal de nóminas dentro del Departamento de Agricultura de Estados Unidos.

Esta falla es distinta a las que fueron abusadas por presuntos agentes de amenazas rusos para comprometer el software SolarWinds Orion que luego se distribuyó a hasta 18 mil de sus clientes, según Reuters.

A fines de diciembre, Microsoft dijo que un segundo grupo de hackers podría haber estado abusando del software Orion del proveedor de infraestructura de TI para colocar una puerta trasera persistente llamada Supernova en los sistemas de destino al aprovechar una vulnerabilidad de omisión de autenticación en la API de Orion para ejecutar comandos arbitrarios.