Descubren otra vulnerabilidad RCE crítica en SolarWinds Orion Platform

Autor: I. Stepanenko

Fecha: Thursday 22nd of April 2021 11:15:15 AM

El proveedor de administración de infraestructura de TI, SolarWinds, lanzó el jueves una nueva actualización de su herramienta de monitoreo de redes Orion con correcciones para cuatro vulnerabilidades de seguridad, contando dos debilidades que podrían ser explotadas por un atacante autenticado para lograr la ejecución remota de código (RCE).

El principal de ellos, es un defecto de deserialización JSON que permite a un usuario autenticado ejecutar código arbitrario a través de la función de acciones de alerta de prueba disponible en Orion Web Console, que permite a los usuarios simular eventos de red (por ejemplo, un servidor que no responde) que se pueden configurar para activar una alerta durante la instalación.

Un segundo problema se refiere a una vulnerabilidad de alto riesgo que un adversario podría aprovechar para lograr RCE en Orion Job Scheduler. *«Para aprovechar esto, un atacante primero necesita conocer las credenciales de una cuenta local sin privilegios en el servidor*

Orion», dijo SolarWinds en sus notas de lanzamiento.

El aviso no contiene muchos detalles técnicos, pero se cree que las dos deficiencias se informaron a través de la iniciativa Zero Day de Trend Micro.

Además de las dos vulnerabilidades mencionadas, la actualización corrige dos errores más, incluyendo una vulnerabilidad de secuencias de comandos de sitios cruzados (XSS) almacenadas de alta gravedad en la pestaña «*agregar pestaña personalizada*», dentro de la página de vista personalizada (CVE-2020-35856) y un tabnabbing inverso y Abrir vulnerabilidad de redireccionamiento en la página de opciones de elementos de menú personalizados (CVE-2021-3109), los cuales requieren una cuenta de administrador de Orion para una explotación exitosa.

La nueva actualización también cuenta con una serie de mejoras de seguridad, con correcciones para prevenir ataques XSS y habilitar la protección UAC para el administrador de bases de datos Orion, entre otros.

La última ronda de correcciones llega casi dos meses después de que la compañía con sede en Texas abordara dos graves vulnerabilidades de seguridad, que afectan a la plataforma Orion (CVE-2021-25274 y CVE-2021-25275), que podrían haverse aprovechado para lograr la ejecución remota de código con privilegios elevados.