Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°251	Fecha: 22-10-2023
		Página: 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Tres vulnerabilidades críticas en SolarWinds		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

   Investigadores de Zero Day Initiative (ZDI) encontraron tres vulnerabilidades críticas de ejecución remota de código en el producto SolarWinds Access Rights Manager (ARM) que los atacantes podrían usar para ejecutar código con privilegios de SYSTEM.

   SolarWinds ARM es una herramienta que permite a las organizaciones administrar y auditar los derechos de acceso de los usuarios en sus entornos de TI. Ofrece integración con Microsoft Active Directory, control de acceso basado en roles, comentarios visuales y más.

2. **DETALLES:**

   A través de la Iniciativa de Día Cero (ZDI) de Trend Micro, los investigadores informaron ocho fallas en la solución SolarWinds el 22 de junio, tres de ellas con gravedad crítica. El proveedor abordó todas las vulnerabilidades a principios de esta semana con un parche disponible en la versión 2023.2.1 de Access Rights Manager.

   A continuación se muestra la descripción y el identificador de las tres ejecuciones remotas de código (RCE) críticas:

   CVE-2023-35182 (gravedad 9,8): Atacantes remotos no autenticados pueden ejecutar código arbitrario en el contexto de SYSTEM debido a la deserialización de datos que no son de confianza en el método "createGlobalServerChannelInternal".

   CVE-2023-35185 (gravedad 9,8): Atacantes remotos no autenticados pueden ejecutar código arbitrario en el contexto de SYSTEM debido a la falta de validación de las rutas proporcionadas por el usuario en el método "OpenFile".

   CVE-2023-35187 (gravedad 9,8): Atacantes remotos no autenticados pueden ejecutar código arbitrario en el contexto de SYSTEM sin autenticación debido a la falta de validación de las rutas proporcionadas por el usuario en el método "OpenClientUpdateFile".

   Ejecutar código en el contexto de "SYSTEM" en Windows significa que se ejecuta con los privilegios más altos en la máquina. SYSTEM es una cuenta interna reservada para el sistema operativo y sus servicios. Los atacantes que obtienen este nivel de privilegios tienen control total sobre todos los archivos en la máquina víctima.

   El resto de los problemas de seguridad que SolarWinds abordó en su Access Right Manager son de alta gravedad y los atacantes podrían explotarlos para aumentar los permisos o ejecutar código arbitrario en el host después de la autenticación.

3. **RECOMENDACIÓN:**

   - Actualizar el producto SolarWinds Access Rights Manager (ARM) con el parche disponible en la versión 2023.2.1.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2023/10/tres-vulnerabilidades-criticas-en.html