Según un aviso publicado ayer por el Centro de Coordinación de CERT, la API de SolarWinds Orion que se utiliza para interactuar con todos los demás productos de gestión y monitoreo del sistema Orion, tiene una vulnerabilidad de seguridad (CVE-2020-10148) que podría permitir que un atacante remoto ejecute sin autenticarse comandos API, lo que resulta en un compromiso de la instancia de SolarWinds.

> *«La autenticación de la API se puede omitir mediante la inclusión de parámetros específicos en la parte Request.PathInfo de una solicitud de URI a la API, lo que podría permitir que un atacante ejecute comandos de API no autenticados»,* dice el aviso.
>
> *«Particularmente, si un atacante agrega un parámetro PathInfo de 'WebResource.adx', 'ScriptResource.adx', 'i18n.ashx' o 'Skipi18n' a una solicitud a un servidor SolarWinds Orion, SolarWinds puede establecer la marca SkipAuthorization, lo que puede permitir que se procese la solicitud de API sin requerir autenticación».*

Cabe mencionar que el aviso de seguridad actualizado de SolarWinds el 24 de diciembre, tomó nota de una vulnerabilidad no especificada en la plataforma Orion que podría explotarse para implementar software malicioso como SUPERNOVA, pero los detalles exactos de la falla no estaban claros hasta ahora.

La semana pasada, Microsoft reveló que un segundo actor de amenazas podría haber estado abusando del software Orion de SolarWinds para lanzar una pieza adicional de malware llamada SUPERNOVA en los sistemas de destino.

También fue corroborado por el equipo de inteligencia de amenazas de la Unidad 42 de las compañías de seguridad Palo Alto Networks y GuidePoint Security, quienes lo describieron como un shell web .NET implementado mediante la modificación de un módulo «app_web_logoimagehandler.ashx.b6031896.dll» de la aplicación SolarWindos Orion.

Si bien el propósito legítimo de la DLL es devolver la imagen del logotipo configurada por un usuario a otros componentes de la aplicación web Orion a través de una API HTTP, las adiciones maliciosas le permiten abrir comandos remotos de un servidor controlado por un atacante y ejecutarlos en memoria en el contexto del usuario del servidor.

> *«SUPERNOVA es novedoso y potente debido a su ejecución en memoria, sofisticación en sus parámetros y ejecución y flexibilidad al implementar una API programática completa en el tiempo de ejecución de .NET»*, dijeron los investigadores de la Unidad 42.

El shell web SUPERNOVA es eliminado por un tercero no identificado diferente de los actores de SUNBURST (rastreado como UNC2452) debido a que la DLL mencionada antes no está firmada digitalmente, a diferencia de la DLL de SUNBURST.

El desarrollo se produce cuando las agencias gubernamentales y los expertos en ciberseguridad están trabajando para comprender todas las consecuencias del hackeo y reconstruir la campaña de intrusión global que potencialmente ha atrapado a 18 mil clientes de SolarWinds.

FireEye, que fue la primera compañía en descubrir el implante SUNBURST, dijo en un análisis que los actores detrás de la operación de espionaje retiraban rutinariamente sus herramientas, incluidas las puertas traseras, una vez que se lograba el acceso remoto legítimo, lo que implica un alto grado de sofisticación técnica y atención a seguridad operacional.

La evidencia descubierta por ReversingLabs y Microsoft había revelado que los bloques de construcción clave para el hack de SolarWinds se implementaron ya en octubre de 2019, cuando los atacantes agregaron una actualización de software de rutina con modificaciones inocuas para combinar con el código original y luego realizaron cambios maliciosos que permitieron para lanzar más ataques contra sus clientes y robar datos.

Para abordar la vulnerabilidad de omisión de autenticación, se recomienda que los usuarios actualicen a las versiones relevantes de la plataforma SolarWinds Orion:

- 2019.4 HF 6 (lanzado el 14 de diciembre de 2020)
- 2020.2.1 HF 2 (lanzado el 15 de diciembre de 2020)
- Parche SUPERNOVA 2019.2 (lanzado el 23 de diciembre de 2020)
- Parche 2018.4 SUPERNOVA (lanzado el 23 de diciembre de 2020)
- 2018.2 Parche SUPERNOVA (lanzado el 23 de diciembre de 2020)

Para los clientes que ya actualizaron a las versiones 2020.2.1 HF2 o 2019.4 HF6, cabe señalar que se han abordado las vulnerabilidades SUNBURST y SUPERNOVA, por lo que no se requieren más acciones.