Alerta de seguridad cibernética	9VSA20-00346-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	28 de diciembre de 2020
Última revisión	28 de diciembre de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Solarwinds por una vulnerabilidad que afecta a su producto Orion. Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidad

CVE-2020-10148

Impacto

La vulnerabilidad CVE-2020-10148 es considerada de riesgo crítico, ya que permite a un atacante remoto el evadir el proceso de autenticación.

La vulnerabilidad existe debido a un error al procesar solicitudes de autenticación dentro de la API al adjuntar un parámetro “PathInfo” a "WebResource.adx", "ScriptResource.adx", "i18n.ashx", o "Skipi18n" a una petición hacia el servidor, en donde Solarwinds podría agregar la bandera “SkipAuthorization”, permitiendo a un atacante no autenticado ejecutar comandos de API los cuales podrían resultar en la instancia de Solarwinds siendo comprometida.

Esta vulnerabilidad ha sido apodada SUPERNOVA y está siendo explotada.

Productos afectados
Solarwinds Orion Platform, versiones de la 2016.1 a la 2020.2.1 HF 1.

Mitigación
Instalar las respectivas actualizaciones desde el sitio del proveedor.

Enlaces
https://www.solarwinds.com/securityadvisory#anchor2

https://www.kb.cert.org/vuls/id/843464

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10148