Alerta de seguridad cibernética	9VSA21-00383-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de febrero de 2021
Última revisión	04 de febrero de 2021

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 de Gobierno, comparte la información sobre vulnerabilidades que afectan a dos productos de SolarWinds, la plataforma Orion y el servidor Serv-U FTP para Windows, que fuera entregada por Trustwave.

Este informe incluye las medidas de mitigación, consistentes en instalar las actualizaciones de los productos afectados.

Vulnerabilidades

CVE-2021-25274
CVE-2021-25275
CVE-2021-25276

Impacto

CVE-2021-25274: Vulnerabilidad que afecta a la plataforma Orion. Un uso inapropiado de Microsoft Messaging Queue puede permitir a un usuario remoto sin privilegios ejecutar código arbitrario con los mayores privilegios.

CVE-2021-25275: Vulnerabilidad que afecta a la plataforma Orion. Debido a que las credenciales de SolarWinds son guardadas de forma insegura, un usuario local, no importando sus privilegios, puede tomar control de la base de datos SOLARWINDS_ORION, robar información o añadir un nuevo nivel de administrador.

CVE-2021-25276: Vulnerabilidad que afecta al servidor Serv-U FTP para Windows. Cualquier usuario local, sin importar sus privilegios, puede crear un archivo que puede definir una nueva cuenta de administrador de Serv-U FTP con acceso total al disco C:\. Esta cuenta puede ser usada para ingresar via FTP y leer o reemplazar cualquier archivo en el disco.

Productos afectados

SolarWinds plataforma Orion
SolarWinds Serv-U FTP para Windows.

Mitigación

Instalar las respectivas actualizaciones desde el sitio del proveedor.

Enlaces

https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/release_notes/orion_platform_2020-2-4_release_notes.htm

https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/full-system-control-with-new-solarwinds-orion-based-and-serv-u-ftp-vulnerabilities/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25274

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25275

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25276