Alerta de seguridad cibernética	9VSA21-00372-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	22 de enero de 2021
Última revisión	22 de enero 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, comparte la información entregada por SolarWinds, sobre vulnerabilidades que afectan a su plataforma Orion y del Orion Network Performance Monitor.

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

Vulnerabilidad

CVE-2020-27871
CVE-2020-27870
CVE-2020-27869
CVE-2020-14005

Impacto

CVE-2020-27871 permite a un usuario remoto realizar ataques de directorio transversal. La vulnerabilidad existe debido a un error de validación de entradas al procesar secuencias de directorio transversal dentro de VulnerabilitySettings.aspx en el SolarWinds Network Performance Monitor. Pese que se exige autenticación para explotar esta vulnerabilidad, el mecanismo de autenticación puede ser evadido.

CVE-2020-27870 posibilita a un atacante remoto ganar acceso no autorizado a información potencialmente sensible en el contexto de la cuenta SYSTEM. La vulnerabilidad tiene lugar debido a una entrega excesiva de datos por parte de la aplicación dentro de ExportToPDF.aspx en el SolarWinds Network Performance Monitor. Se requiere autenticación para explotar esta vulnerabilidad.

CVE-2020-27869 hace posible a un usuario remoto ejecutar solicitudes SQL arbitrarias en la base de datos, debido a una sanitización insuficiente de los datos entregados por el usuario dentro del método WriteToFile en SolarWinds Network Performance Monitor. La explotación exitosa de esta vulnerabilidad permitiría a un atacante remoto escalar privilegios y resetear la contraseña del usuario Administrador.

CVE-2020-14005 permite a un usuario remoto comprometer el sistema afectado, gracias a una insuficiente validación de la información ingresada por el usuario dentro de los métodos ExecuteVBScript y ExecutrExternalProgram en SolarWinds Performance Monitor. Un usuario remoto autenticado puede ingresar datos especialmente diseñados a la aplicación y ejecutar código arbitrario con privilegios SYSTEM.

Productos Afectados

Orion Platform, versiones de la 2019.2 a la 2020.2.1 HF 1.
Orion Network Performance Monitor, versiones de la 2019.4 a la 2020.2 Hotfix 1.

Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

Enlaces

https://www.zerodayinitiative.com/advisories/ZDI-21-063/

https://www.zerodayinitiative.com/advisories/ZDI-21-064/

https://www.zerodayinitiative.com/advisories/ZDI-21-066/

https://www.zerodayinitiative.com/advisories/ZDI-21-067/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27871

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27870

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27869

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14005

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.01.22 18:20:02 -03'00'