Alerta de seguridad cibernética	9VSA21-00434-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	01 de mayo de 2021
Última revisión	01 de mayo 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 información sobre dos vulnerabilidades zero day en Parallels Desktop.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-31424
CVE-2021-31427

Impactos

CVE-2021-31427: Esta vulnerabilidad, que existe dentro del componente Open Tools Gate, permite a atacantes locales revelar información sensible en instalaciones afectadas de Parallels Desktop 15.1.5-47309. Para poder explotar esta vulnerabilidad, el atacante debe primero obtener la habilidad de ejecutar código de bajos privilegios en el sistema objetivo.

CVE-2021-31424: Esta vulnerabilidad permite a un usuario local ejecutar código arbitrario en el sistema objetivo, debido a un error dentro del componente Open Tools Gate. Un usuario local puede entregar datos especialmente diseñados a la aplicación, detonar un error de desbordamiento de buffer y ejecutar código arbitrario en el sistema objetivo, resultando en su total compromiso.

Productos Afectados

Parallels Desktop 15.1.5-47309

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor. La actualización será hecha disponible en https://kb.parallels.com/en/125013.

Enlaces

https://kb.parallels.com/en/125013
https://www.zerodayinitiative.com/blog/2021/4/26/parallels-desktop-rdpmc-hypercall-interface-and-vulnerabilities
https://www.zerodayinitiative.com/advisories/ZDI-21-435/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31424
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31427

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.01 12:34:38 -04'00'