Alerta de seguridad informática	9VSA-00073-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de octubre de 2019
Última revisión	22 de octubre de 2019

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 Avira, referente a una vulnerabilidad en su software de actualización, junto a su respectiva forma de mitigarla.

Vulnerabilidad

CVE-2019-17449

Impacto

Es posible realizar ejecución de código, escalación de privilegios, evasión de sistemas de seguridad y persistencia, inyectando un archivo DLL en una de las carpetas de configuración de Avira. Esto ocurre ya que al iniciar Avira.ServiceHost.exe, intenta cargar el archivo Windtrust.dll, el cual puede ser sustituido utilizando los privilegios de administrador. Finalmente, Avira firma este DLL malicioso como si fuera propio.

Productos Afectados

Avira Software Updates versiones anteriores a la 2.0.6.21094

Mitigación

Actualizar a la versión 2.0.5.21245, el enlace para actualizar se encuentra al final de este documento.

Enlace

- https://support.avira.com/hc/en-us/articles/360000142857-Avira-Software-Updater
- https://nvd.nist.gov/vuln/detail/CVE-2019-17449

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.22 11:07:49 -03'00'