Alerta de seguridad informática	9VSA20-00170-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de abril de 2020
Última revisión	03 de abril 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 Avast referente a múltiples vulnerabilidades que afectan a su antivirus. El presente informe incluye las respectivas medidas de mitigación.

VULNERABILIDADES

CVE-2020-10868
CVE-2020-10867
CVE-2020-10866
CVE-2020-10865
CVE-2020-10864
CVE-2020-10863
CVE-2020-10862
CVE-2020-10861
CVE-2020-10860

CVE-2020-10868

Impacto

Debido a restricciones de acceso inadecuadas en el endpoint “aswTask RPC” para la librería “TaskEx” en el servicio Avast (AvastSvc.exe), un atacante remoto podía eludir estas restricciones implementadas y ejecutar “Repair APP RPC” desde un proceso de baja integridad.

CVE-2020-10867

Impacto

Debido a restricciones de acceso inadecuadas en el endpoint “aswTask RPC” para la librería “TaskEx” en el servicio Avast (AvastSvc.exe), un atacante remoto podía eludir estas restricciones y obtener acceso no autorizado a la aplicación.

CVE-2020-10866

Impacto

Debido a restricciones de acceso inadecuadas en el endpoint “aswTask RPC” para la librería “TaskEx” en el servicio Avast (AvastSvc.exe), un atacante remoto podía eludir estas restricciones y enumerar las interfaces de red y los APs (Access points) desde un proceso de baja integridad via RPC.

CVE-2020-10865

Impacto

Debido a restricciones de permisos inadecuadas en el endpoint “aswTask RPC” para la librería “TaskEx” en el servicio Avast (AvastSvc.exe), un atacante podía evadir medidas de seguridad implementadas y realizar cambios arbitrarios a la sección “Components” del archivo “Stats.ini” vía RPC desde un proceso de baja integridad.

CVE-2020-10864

Impacto

Debido a la insuficiente validación de datos entregados por el usuario en el endpoint “aswTask RPC” para la librería “TaskEx” en el servicio Avast (AvastSvc.exe), un atacante podía gatillar un reboot vía RPC desde un proceso de baja integridad

CVE-2020-10863

Impacto

Debido a la insuficiente validación de datos entregados por el usuario en el endpoint “aswTask RPC” para la librería “TaskEx” en el servicio Avast (AvastSvc.exe), un atacante podía gatillar una señar de apagado vía RPC desde un proceso de baja integridad

CVE-2020-10862

Impacto

Debido a validaciones de permisos inadecuadas en el endpoint “aswTask RPC” para la librería “TaskEx” en el servicio Avast (AvastSvc.exe), un atacante podía obtener privilegios elevados vía RPC en el sistema afectado.

CVE-2020-10861

Impacto

Debido a restricciones de permisos inadecuadas en el endpoint “aswTask RPC” para la librería “TaskEx” en el servicio Avast (AvastSvc.exe), un atacante podía evadir medidas de seguridad implementadas y eliminar archivos arbitrarios del Avast Program Path vía RPC, cuando “Self Defense” estaba activado.

CVE-2020-10860

Impacto
Debido a un error en memoria en la librería “aswAvLog”, un atacante remoto podía gatillar este error y causar una denegación de servicios en los sistemas afectados.

Productos Afectados
Avast antivirus versiones anteriores a la 20.

Mitigación
Actualizar a la versión más reciente (la versión 20.2.2401).

Enlace
https://forum.avast.com/index.php?topic=232420.0
https://forum.avast.com/index.php?topic=232423.0
https://github.com/umarfarook882/Avast_Multiple_Vulnerability_Disclosure/blob/master/README.md
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10868
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10867
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10866
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10865
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10864
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10863
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10862
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10861
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10860

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.03 09:10:28 -03'00'