Alerta de seguridad informática	9VSA-00082-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de noviembre de 2019
Última revisión	06 de noviembre 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 información obtenida de diferentes fuentes, referente a dos vulnerabilidades que afectan al Antivirus de Avast, las cuales, si son explotadas, pueden resultar en una denegación de servicios o en un ataque remoto XSS (Cross-site Scripting). También se entrega información sobre su respectiva actualización para mitigar los riesgos.

Vulnerabilidad

- CVE-2019-18653
- CVE-2019-11230

Impacto

Por causa de una deficiente sanitización del SSID en la notificación de red que genera el antivirus, un atacante remoto podría generar un ataque XSS, a través de código HTML y JavaScript, en el cual el atacante podría robar información sensible, cambiar la apariencia del sitio web, realizar ataques de phishing e inducir descargas de malware.

Producto Afectado

Avast Antivirus versión 19.3.2369 build 19.3.4241.440.

Mitigación

Actualizar a la versión más reciente del antivirus.

Enlaces

- https://nvd.nist.gov/vuln/detail/CVE-2019-18653

Impacto

Es posible realizar una denegación de servicios local de manera autenticada, renombrando archivos arbitrarios al reemplazar Logs/Update.log con un symlink. Cuando el antivirus intente escribir sobre el archivo de logs, el destino del symlink es renombrado. Este defecto se puede explotar renombrando archivos críticos como AvastSvc.exe, causando una falla la próxima vez que se inicie el sistema.

Producto Afectado

Avast Antivirus versiones 12.1.2272, 12.2.2276, 12.3.2279, 17.1.2286, 17.2.2288, 17.3.2290, 17.3.2291, 17.4.2294, 17.5.2302, 17.6.2310, 17.7.2314, 17.8.2318, 17.9.2322, 18.1.2326, 18.2.2328, 18.3.2333, 18.4.2338, 18.5.2342, 18.6.2349, 18.7.2354, 18.8.2356, 19.1.2360, 19.2.2364, 19.3.2369, 2015.10.4.2233, 2016.11.1.2241, 2016.11.1.2245, 2016.11.1.2253, 2016.11.1.2260, 2016.11.1.2261, 2016.11.1.2262.

Mitigación

Actualizar a la versión más reciente del antivirus.

Enlaces

- https://nvd.nist.gov/vuln/detail/CVE-2019-11230

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.06 11:50:54 -03'00'