Alerta de seguridad informática	9VSA-00040-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de agosto de 2019
Última revisión	30 de agosto 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 recopilada desde diferentes fuentes[1] referente a una vulnerabilidad detectada en el cliente STEAM de VALVE, y las respectivas recomendaciones para mitigar el riesgo.

[1] Fueron consultadas https://www.mitre.org y https://www.nist.gov, entre otras.

Vulnerabilidad

CVE-2019-13516

Impacto

A través de un uso específico para CreateMountPoint.exe y SetOpLock.exe, se aprovecha los débiles permisos de carpeta que tiene STEAM para escalar privilegios en WINDOWS (a NT AUTHORITY\SYSTEM) aprovechando una condición de TOCTOU.

Productos Afectados

Todas las versiones antes anteriores al 26-08-2019.

Mitigación

Instalar la actualización indicada por VALVE (26-08-2019).

Enlaces:

- https://store.steampowered.com/news/?feed=steam_client (**actualización**)
- https://unaaldia.hispasec.com/2019/08/elevacion-de-privilegios-local-en-el-cliente-steam-para-windows.html
- https://nvd.nist.gov/vuln/detail/CVE-2019-15316
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15316
- https://steamcommunity.com/groups/SteamClientBeta/announcements/detail/1599262071399843693

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.08.30 20:02:50 -04'00'