Alerta de seguridad informática	9VSA20-00144-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de febrero de 2020
Última revisión	19 de febrero 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 información obtenida de múltiples fuentes, referente a una vulnerabilidad que afecta al videojuego DOTA 2 de Valve, la cual de ser explotada, permitiría a un atacante realizar ataques de denegación de servicios y ejecución de código remoto. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2020-9005

Impactos

Un atacante podría realizar ataques de denegación de servicios o ejecutar código de forma arbitraria en el sistema afectado debido a la insuficiente validación de datos ingresados por el usuario en el archivo “meshsystem.dll”, en la función “GetValue”. Un atacante remoto podría crear un mapa especialmente diseñado e invitar a la víctima a este para realizar la ejecución del ataque.

Productos Afectados

Esta vulnerabilidad afecta a todas las versiones de DOTA 2 hasta la versión 2.7.24.

Mitigación

Se debe actualizar a la versión más reciente siguiendo las indicaciones del fabricante.

Enlaces

https://www.cybersecurity-help.cz/vdb/SB2020021815
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9005

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.19 16:52:13 -03'00'