Un actor de amenazas desconocido creó modos de juego maliciosos para el videojuego de campo de batalla en línea multijugador (MOBA) de Dota 2, que podría haberse aprovechado para establecer acceso de puerta trasera a los sistemas de los jugadores.

Los modos explotaron una vulnerabilidad de alta gravedad en el motor JavaScript V8 rastreado como CVE-2021-38003 (puntaje CVSS: 8.8), que fue explotado como un día cero y Google lo abordó en octubre de 2021.

> *«Debido a que V8 no estaba aislado en Dota, el exploit por sí solo permitió la ejecución remota de código contra otros jugadores de Dota»,* dijo el investigador de Avast, Jan Vojtěšek.

Después de la divulgación responsable a Valve, el editor del juego envió correcciones el 12 de enero de 2023 al actualizar la versión de V8.

Los modos de juego son esencialmente capacidades personalizadas que pueden mejorar un título existente u ofrecer un juego completamente nuevo de una forma que se desvía de las reglas estándar.

Aunque la publicación de un modo de juego personalizado en la tienda Steam incluye un proceso de investigación de Valve, los modos de juego maliciosos descubiertos por el proveedor de antivirus lograron pasar desapercibidos.

Estos modos de juego, que desde entonces han sido eliminados, son «test addon please ignore», «Overdog no annoying heroes», «Custom hero fight» and «Overthrow RTZ Edition X10 XP». También se cree que el atacante publicó un quinto modo de juego llamado Brawl en Petah Tiqwa que no incluía ningún código malicioso.

Incrustado dentro de *«test addon plz ignore»* hay un exploi para la falla V8 que podría armarse para ejecutar shellcode personalizado.

Los otros tres, por otro lado, adoptan un enfoque más encubierto en el que el código malicioso está diseñado para llegar a un servidor remoto para obtener una carga útil de JavaScript, que también es probable que sea la vulnerabilidad CVE-2021-38003 desde el servidor ya no accesible.

En un escenario de ataque hipotético, un jugador que inicia uno de los modos de juego anteriores podría ser atacado por el hacker para lograr el acceso remoto al host infectado e implementar malware adicional para una mayor explotación.

No se sabe de inmediato cuáles fueron los objetivos finales del desarrollador detrás de la creación de los modos de juego, pero es poco probable que sean para fines de investigación benignos, dijo Avast.

> *«Primero, el atacante no informó la vulnerabilidad a Valve (lo que generalmente se consideraría algo agradable). En segundo lugar, el atacante trató de ocultar el exploit en una puerta trasera sigilosa»*, dijo Vojtěšek.

> *«Independientemente, también es posible que el atacante tampoco tuviera intenciones puramente maliciosas, ya que podría decirse que dicho atacante podría abusar de esta vulnerabilidad con un impacto mucho mayor».*