Vulnerabilidades críticas en una biblioteca de red central que impulsa la funcionalidad de juegos en línea de Valve, podría haber permitido a los actores maliciosos bloquear los juegos de forma remota e incluso, tomar el control de los servidores de juegos de terceros afectados.

> *«Un atacante podría bloquear de forma remota el cliente de juego de un oponente para forzar una victoria o incluso realizar un 'abandono de la ira nuclear' y bloquear el servidor de juego de Valve para terminar el juego completamente. Potencialmente aún más dañino, los atacantes podrían apoderarse de forma remota de servidores de juegos de desarrolladores de terceros para ejecutar código arbitrario»*, dijo Eyal Itkin de Check Point Research.

Valve es un popular desarrollador y editor de juegos con sede en Estados Unidos. Detrás de la plataforma de distribución de software de juegos Steam y de distintos títulos como Half-Life, Counter-Strike, Portal, Day of Defeat, Team Fortress, Left 4 Dead y Dota.

Las cuatro vulnerabilidades (CVE-2020-6016 a CVE-2020-6019) se descubrieron en la biblioteca Game Networking Sockets (GNS) o Steam Sockets de Valve, una biblioteca de redes de código abierto que proporciona una *«capa de transporte básica para juegos»,* lo que permite una combinación de funciones UDP y TCP con soporte para encriptación, mayor confiabilidad y comunicaciones peer-to-peer (P2P).

Steam Sockets también se ofrece como parte del Steamworks SDK para desarrolladores de juegos de terceros, con las vulnerabilidades encontradas tanto en los servidores Steam como en sus clientes instalados en los sistemas de los jugadores.

El ataque depende de una falla específica en el mecanismo de reensamblaje de paquetes (CVE-2020-6016) y una peculiaridad en la implementación de iteradores de C++ para enviar un montón de paquetes maliciosos a un servidor de juego de destino y desencadenar un desbordamiento de búfer basado en montón, lo que finalmente causa que el servidor aborte o se bloquee.

Luego de la divulgación responsable a Valve el 2 de septiembre de 2020, las actualizaciones binarias que contienen las correcciones se enviaron a los clientes y servidores del juego de Valve el 17 de septiembre.

Pero Check Point Research asegura que algunos desarrolladores de juegos de terceros aún no han parcheado sus clientes a partir del 2 de diciembre.

> *«Los videojuegos han alcanzado un máximo histórico durante la pandemia de coronavirus. Con millones de personas que juegan juegos en línea actualmente, incluso el más mínimo problema de seguridad puede ser una preocupación seria para las empresas de juegos y la privacidad de los jugadores. A través de las vulnerabilidades que encontramos, un atacante podría haberse apoderado de cientos de miles de computadoras para jugadores todos los días, con las víctimas completamente ciegas»,* dijo Itkin.

> *«Las plataformas en línea populares son un buen terreno de recolección para los atacantes. Siempre que hay millones de usuarios que inician sesión en el mismo lugar, el poder de un exploit sólido y confiable aumenta exponencialmente»*, agregó.

Check Point también mencionó que los jugadores de Valve a través de Steam ya están protegidos por la solución, aunque los jugadores de juegos de terceros deben asegurarse de que sus clientes reciban una actualización en los últimos meses para mitigar el riesgo asociado con la falla.