Investigadores de seguridad cibernética revelaron una vulnerabilidad de lectura fuera de los límites en el lenguaje de programación Squirrel, que los atacantes pueden abusar para eliminar las restricciones de la zona de pruebas y ejecutar código arbitrario dentro de un SquirrelVM, lo que brinda a un actor malintencionado acceso completo a la máquina subyacente.

Rastreada como CVE-2021-41556, la falla ocurre cuando una biblioteca de juegos denominada Squirrel Engine se utiliza para ejecutar código que no es de confianza y afecta las ramas de versión estable 3.x y 2.x de Squirrel. La vulnerabilidad se reveló de forma responsable el 10 de agosto de 2021.

Squirrel es un lenguaje de programación de código abierto orientado a objetos que se utiliza para crear scripts de videojuegos y también en dispositivos IoT y plataformas de procesamiento de transacciones distribuidas como Enduro/X.

> *«En un escenario del mundo real, un atacante podría incrustar un script Squirrel malicioso en un mapa de la comunidad y distribuirlo a través del Steam Workshop de confianza. Cuando el propietario de un servidor descarga e instala este mapa malicioso en su servidor, se ejecuta el script Squirrel, escapa de su VM y toma el control de la máquina del servidor»*, dijeron los investigadores Simon Scannell y Niklas Breitfeld en un informe compartido con Masterhacks.

El problema de seguridad identificado se refiere a un *«acceso fuera de los límites a través de la confusión del índice»* al definir clases de Squirrel que podrían explotarse para secuestrar el flujo de control de un programa y obtener el control total de la máquina virtual de Squirrel.

Aunque el problema ya se abordó como parte de una confirmación de código enviada el 16 de septiembre, cabe mencionar que los cambios no se han incluido en una nueva versión estable, con la última versión oficial (v3.1) lanzada el 27 de marzo de 2016.