Desbordamiento de búfer

Es una anomalía que se produce cuando el software que escribe datos en un búfer desborda la capacidad del búfer, lo que provoca que se sobrescriba las ubicaciones de memoria adyacentes. Los ciberdelincuentes se aprovechan de esta anomalía con el objetivo de modificar la memoria de un ordenador para socavar o tomar el control de la ejecución del programa.

¿Qué es un búfer?

Es un área de almacenamiento de memoria física que se utiliza para almacenar temporalmente los datos mientras se trasladan de un lugar a otro. Estos búferes suelen estar en la memoria RAM.

¿Cómo se aprovechan de esto?

Introducir deliberadamente una entrada cuidadosamente elaborada en un programa que provocará que este intente almacenar esa entrada en un búfer que no sea lo suficientemente grande, sobrescribiendo partes de la memoria conectadas al espacio del búfer.

Ejemplos

Ataque de desbordamiento de la pila/ Stack buffer overflow attack *

Es el tipo más común en esta rama y consiste en desbordar el búfer en la pila de llamadas o stack de memoria.

Ataque de desbordamiento del montón/ Heap buffer overflow attack*

Tiene como objetivo los datos en la reserva de memoria abierta conocida como montón.

Ataque de desbordamiento de enteros/ Integer overflow attack

En si, no es un desbordamiento de búfer directamente, pero puede conducir a él. Esto ocurre cuando una operación aritmética produce un resultado mayor que el máximo valor que puede almacenar un tipo de dato entero.

Desbordamiento de Unicode/ Unicode overflow

Crea un desbordamiento de búfer al insertar caracteres Unicode en una entrada que espera caracteres ASCII.

Los computadores se basan en 2 modelos diferentes de asignación de memoria, conocidos como la pila y el montón, ambos están situados en la memoria RAM.