Buffer overflow

This is an anomaly that occurs when software writing data to a buffer overflows the buffer's capacity, causing adjacent memory locations to be overwritten. Cybercriminals take advantage of this anomaly in order to modify a computer's memory to undermine or take control of the program's execution.

What is a buffer?

It is a physical memory storage area used to temporarily store data while it is being moved from one place to another. These buffers are usually located in RAM.

How do they take advantage of this?

Deliberately introducing carefully crafted input into a program that will cause it to attempt to store that input in a buffer that is not large enough, overwriting parts of memory connected to the buffer space.

Examples

Stack buffer overflow attack

This is the most common type in this branch and consists of overflowing the buffer in the call stack or memory stack.

Heap buffer overflow attack

Targets data in the open memory pool known as the heap.

Integer overflow attack

Not a buffer overflow per se, but can lead to one. This occurs when an arithmetic operation produces a result larger than the maximum value that an integer data type can store.

Unicode overflow

Creates a buffer overflow by inserting Unicode characters into an input that expects ASCII characters.