BUFFER OVERFLOW

CSCI 330

Professor Hill

Jenny MIN

What is Buffer Overflow?

Buffer Overflow is also known as buffer overrun in Information security and programming

Buffer overflow is an anomaly where a program overruns the buffer's boundary and overwrites adjacent memory locations.

Buffer overflow is one of the popular software security vulnerabilties that is very common

What Type of Vulnerability is Buffer Overflow?

Buffer overflow has an vulnerability of a software coding error.

How Does Buffer Overflow Work?

A buffer overflow attack typically involves violating programming languages and overwriting the bounds of the buffers they exist on. Most buffer overflows are caused by the combination of manipulating memory and mistaken assumptions around the composition or size of data.

The software error focuses on buffers, which are sequential sections of computing memory that hold data temporarily as it is transferred between locations.

It occurs when the amount of data in the buffer exceeds its storage capacity. That extra data overflows into adjacent memory

When Does Buffer Overflow Happens?

1. reliant on external data to control its behavior
2. dependent on data properties that are enforced beyond its immediate scope
3. complex that programmers are not able to predict its behavior accurately

How can we prevent buffer overflows?

Modern operating systems now deploy runtime protection that enables additional security against buffer overflows.

1. Address space layout randomization (ASLR)
2. Data execution prevention
3. Structured exception handling overwrite protection (SEHOP)

How concerned should we be?

By experiencing buffer overflow, it can be exploited by hacker to gain unauthorized access to corporate systems.

1. System crashes
2. Access control loss
3. Further security issues