

Esercizio Epicode 09.11.2023

Buffer Overflow

Per evitare sia l'errore **segmentation fault** che il **bus error**, sostituiamo il comando **scanf** con **fgets** cosicché l'input dato dall'utente si fermi rispetto al valore char della variabile buffer (in questo caso 30). Se l'utente digita più di 30 caratteri, l'output ridato prenderà solo i primi 30.

Segmentation fault

Quest'errore si verifica quando un programma tenta di accedere a un'area di memoria che non gli appartiene. Questa area di memoria può essere non inizializzata, liberata o riservata a un altro processo.

Bus error

Quest'errore si verifica quando un programma tenta di accedere a un'area di memoria che è protetta. Questa area di memoria può essere riservata al sistema operativo o a un altro dispositivo hardware.

Questi due errori sono vulnerabili ai seguenti attacchi:

- Buffer overflow: Un possibile black hat potrebbe fornire un input che sia più lungo del buffer previsto. Questo potrebbe causare un errore segmentation fault o un errore bus error se il programma tenta di scrivere oltre il limite del buffer.
- Esecuzione di codice arbitrario: Un black hat potrebbe fornire un input che contenga codice arbitrario. Se il programma tentasse di eseguire il codice arbitrario, questo potrebbe essere eseguito con i privilegi del programma.
- Denial-of-service: Un utente black hat potrebbe fornire un input che causi un errore segmentation fault o un errore bus error in modo ripetuto. Questo potrebbe portare al crash del sistema o dell'applicazione.