

**Segurança de Sistemas Informáticos**

**Ficha de Exercícios 3 – Information Security**

**Grupo 04**

**2022/2023**

Esta ficha de exercícios tem por objetivo principal analisar e corrigir erros de programas escritos na linguagem de programação C, usando como guia de erros o Top 25 CWE (Common Weakness Enumeration).

Uma imagem com pessoa, pousar

Descrição gerada automaticamente 

A91697 - Luís Filipe Fernandes Vilas A91671 - João Manuel Novais da Silva

**Exercício 1:**

Uma imagem com texto

Descrição gerada automaticamenteNeste programa rapidamente é pressentível que existe uma violação da integridade do sistema, uma vez que a linha “arr[index] = value;” está a escrever o valor de “value” numa posição da memória que não foi alocada para o intuito do programa. Por isso estamos num caso de duma falha do tipo CWE-787 Out-of-bounds Write, pois estamos a escrever informação depois do final do limite do buffer alocado, com isto é possível corromper os dados, provocar crashes ou até manipular o funcionamento do sistema para ser explorado por atacantes.

Logo para arranjarmos este problema podemos reescrever o código de maneira ou alterar o valor de “index” para 4 ou para o tamanho do array anteriormente alocado. Caso o objetivo deste código fosse acrescentar um novo elemento no final do array teríamos que realocar memória para um novo array com espaço para mais um inteiro.

Uma imagem com texto

Descrição gerada automaticamente

**Exercício 2:**

**Uma imagem com texto

Descrição gerada automaticamente**

Para este caso é possível ver que existe a possibilidade da violação da Confidencialidade e Acessibilidade do sistema uma vez que a função “open()”, como descrito no manual, necessita de receber uma flag que indique as permissões, porém isto não é obrigatório, no caso de não serem fornecidas as permissões a atribuição destas é feita pelo compilador. Neste caso, usando uma máquina com Windows11 todos os utilizadores têm permissões de escrever, ler e executar o ficheiro “file.txt”. Isto poderá comprometer a segurança do utilizador pois qualquer utilizador da máquina tem acesso ao ficheiro, cujo pode conter informações importantes. Logo estamos num caso duma fraqueza do tipo CWE-276 Incorrect Default Premissions.

Para concertar este programa podemos definir as permissões:

Uma imagem com texto

Descrição gerada automaticamente

**Exercício 3:**

Uma imagem com texto

Descrição gerada automaticamenteO terceiro programa apresenta uma vulnerabilidade que pode comprometer a Integridade e Acessibilidade do sistema, devido ao facto de alocação de memória para o array “arr” ser da escolha do utilizador. Por isso, o utilizador pode introduzir um valor inteiro que seja maior do que o limite máximo da linguagem, originado assim no Integer Overflow ou num Wraparound fazendo com que o valor utilizado na função malloc não seja o que o utilizador pretendia podendo ser este um valor muito pequeno ou até negativo. Com isto é possível ver um caso em que seja alocado uma lista de tamanho pequena, mas o programa assuma que esta é grande originando em problemas Out-of-Bounds (CWE-119).

Assim, temos aqui fraquezas do tipo CWE-190 Integer Overflow or Wraparound e também CWE-20 Improper Input Validation que pode resultar em corrupção de dados, comportamentos não esperados, loops infinitos e crashes do sistema.

Para resolver este problema podemos fazer apenas uma simples verificação se o valor introduzido é demasiado grande ou negativo:

Uma imagem com texto

Descrição gerada automaticamente

**Uma imagem com texto

Descrição gerada automaticamenteExercício 4:**

Finalmente, no programa 4 é possível verificar que, mais uma vez, temos a necessidade de input do utilizador, podendo originar na exploração de vulnerabilidades por um atacante. Neste caso alocamos 20 bytes de memória para a variável “username” mas depois valos dar-lhe o valor do input do utilizador, por isso, se o utilizador inserir mais do que 20 caracteres podemos correr riscos de violar a Integridade e Acessibilidade do sistema.

Temos aqui duas fraquezas do tipo CWE-787 Out-of-bounds Write e CWE-798 Hard-coded Credentials, no sentido em que a palavra-passe do utilizador é fixada no programa.

Para corrigirmos estes problemas podemos passar por apenas alocar memória às variáveis que vão guardar os dados no momento em que recebemos o input, assegurando que assim, alocamos a memória necessária para o input, e também pedir ao utilizador para introduzir a sua palavra-passe.

Uma imagem com texto

Descrição gerada automaticamente