1- Vulnerabilidade de codificação

Pergunta 1.1

O número de linhas de código que aparecem no site https://informationisbeautiful.net/visualizations/million-lines-of-code/ são:

- Facebook tem 61 milhões,
- Software de automóveis tem 100 milhões,
- Linux 3.1 tem 15 milhões,
- Google tem 2 mil milhões.

Tendo por base o número de linhas de código e o que aprendemos nas aulas, sabe-se que por cada mil linhas de código existem entre 5 a 50 bugs. Logo, temos que

- Facebook tem entre 300 mil a 3 milhões de bugs,
- Software de automóveis tem entre 500 mil a 5 milhões de bugs,
- Linux 3.1 tem entre 75 mil a 750 mil de bugs,
- Google tem entre 10 milhões a 100 milhões de bugs.

Não sabemos ao certo quantos destes bugs são vulnerabilidades, no entanto podemos dizer no máximo o número de vulnerabilidades é igual ao número de bugs.

Pergunta 1.2

Vulnerabilidades de projeto são, por exemplo, **CWE-656: Reliance on Security Through Obscurity**, onde para corrigir bastaria usar métodos conhecidos seguros, e **CWE-327: Use of a Broken or Risky Cryptographic Algorithm**, onde para corrigir bastaria utilizar um algoritmo criptográfico mais seguro.

Vulnerabilidades de codificação são, por exemplo, **CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**, onde para corrigir bastaria invalidar todos os *inputs* não validados, e **CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')**, onde para corrigir bastaria criar blocos de código sincronizados.

Vulneranilidades operacionais são, por exemplo, **CWE-13: ASP.NET Misconfiguration: Password in Configuration File**, onde para corrigir bastaria cifrar as credenciais do utilizador, e **CWE-520: .NET Misconfiguration: Use of Impersonation**, havendo premissões mais altas a utilizadores que não era suposto, bastaria limitar as permissões a níveis mais baixos do sistema de ficheiros.

Pergunta 1.3

As vulnerabilidades dia-zero são vulnerabilidades que ainda não são conhecidas pelas entidades interessadas em corrigi-las. Desta forma, se houver um ataque usando estas vulnerabilidades é muito mais difícil de resolver, uma vez que como estas ainda não foram expostas vai demorar mais tempo até em primeiro lugar se descubra a vulnerabilidade, até que por fim se possa resolvê-la.