CWE-502: Deserialization of Untrusted Data

Desserialização de dados não confiáveis

Alexandre Thurow
Gabriel Todesco

O que é?

- A aplicação desserializa dados não confiáveis sem verificar se eles são realmente válidos;
- É muito comum serializar objetos para comunicação ou armazenamento para um uso posterior;
- Dados desserializados podem ser modificados por funções impróprias, se não usar criptografia para protegê-los;
- Segurança do cliente.

Dados que não são confiáveis, não podem ser confiáveis para virarem informação.

Fases do desenvolvimento onde pode ser gerada

1. Ocorre quando deixa-se de implementar uma tática de segurança durante a fase de **Arquitetura e Design**.

2. **Implementação**.

Como é explorada

- Desenvolvedores não impõem restrições às “cadeias de gadgets” ou a instâncias e invocações de métodos;
- Invasores podem utilizá-los para executar ações não autorizadas;
- Ex: gerar interações com os serviços do sistema operacional.

Probabilidade de exploração: **Média**.

Consequências

- Integridade: os invasores podem modificar objetos ou dados inesperados que foram considerados seguros contra modificações;

- Disponibilidade: se uma função está esperando uma condição para terminar, possivelmente ela nunca termine;

- Podem variar, pois depende dos objetos ou métodos são desserializados e usados;

- Portanto, assumir que o código no objeto desserializado é perigoso e pode permitir a exploração.

Plataformas aplicáveis

- Java;
- Ruby;
- PHP;
- Python;
- Javascript.

Redução dos prejuízos causados

- Utilizar recursos da linguagem de programação;
- Novo objeto;
- Definir um estado final no objeto;
- Tornar campos transitórios;
- Evitar permitir dispositivos desnecessários de terem acesso ao sistema.

DEMONSTRAÇÃO