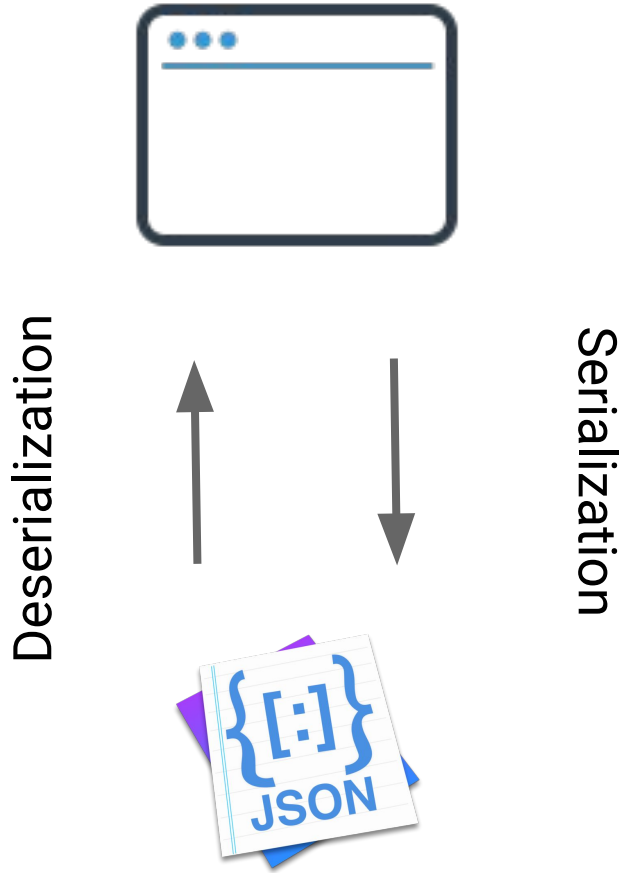
CWE-502: Deserialization of Untrusted Data

Acadêmicos: Adriner M. de Andrade
Christian Passold

Descrição do problema

O sistema executa a ação de desserializar um objeto qualquer sem fazer as devidas validações, sendo assim, o arquivo pode conter dados maliciosos ao sistema.

Descrição do problema



Aspectos de segurança afetados

- **Integridade**
  - *Modify Application Data*
- **Disponibilidade**
  - *DoS: Resource Consumption (CPU)*
- **Outros**
  - Depende do uso da aplicação

Exemplo

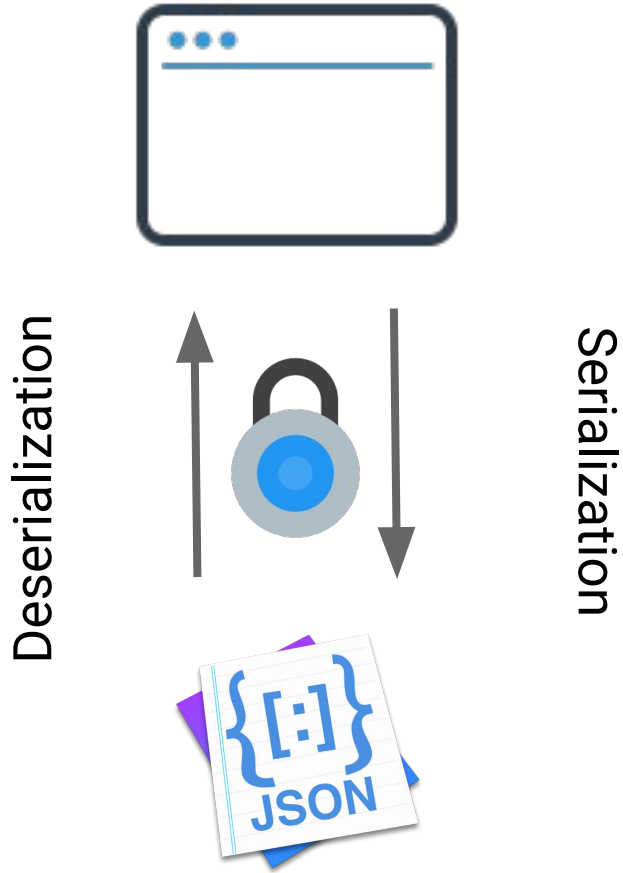
```
try {
        File file = new File("object.obj");
        ObjectInputStream in = new
        ObjectInputStream(new
        FileInputStream(file));
        javax.swing.JButton button =
        (javax.swing.JButton)
        in.readObject();
        in.close();
}
```

Fonte: https://cwe.mitre.org/data/definitions/502.html

Algumas soluções possíveis

- Criptografia
  - Encriptar o arquivo é uma opção para que não haja alterações no código
- SHA Hash
  - Com isso é possível verificar qualquer alteração feita no arquivo após sua criação.
- Outros

Criptografia



Aplicação exemplo