Insecure Deserialization

Insecure Deserialization is a vulnerability that uses untrusted data to attack an application and cause a Denial of Service (DoS) attack or execute a malicious code upon being deserialized.

3 main types

1. Blind deserialization attacks

* Attacks that happen behind restricted firewall protected networks by exploiting payloads or manipulating chain of Transformers

1. Asynchronous deserialization attacks
   * Attack that stores serialized gadgets in databases then attacks when a target application deserializes
   * Uses a sequence of ROP (return-oriented programming) gadget that end in RET (return from procedure) instruction.
2. Deferred-execution deserialization
   * Uses a sequence of ROP (return-oriented programming) gadget that end in RET (return from procedure) instruction.
   * bypasses non-executable page protections like read-only memory and kernel-code cohesion protections

Protection

1. Blacklisting – deny access to sensitive that are unsafe
2. Whitelisting – allow access to exclusive users, domains and softwares

Both ways of protection should be used to have a better protection