**A8 unsichere Deserialisierung**

Serialisierung ist den Zustand eines Objektes vollständig in einen Bytestrom zu verwandeln um eine leichte bzw. um eine Übertragung zu ermöglichten.

Deserialisierung ist der Vorgang aus dem Bytestrom (Bytes) wieder das Objekt zu erstellen

* **Leicht Verwundbar, wenn**
  + Daten ohne irgendwelche Überprüfung empfangen werden
  + Keine Abbruchkriterien beim empfangen von Daten vorliegen
  + Daten die Serialisiert werden keine Einschränkung der Zugriffsrechte besitzen
* **Beispiel Attacke „Deserialisierte Daten“**
  + Serialisierung löst eine Aktion aus die Schaden anrichtet
  + Serialisierung blockiert die Leitung und verhindert weiteren Zugriff
  + Serialisierung erlaubt Zugriff des Angreifers aufs Opfersystem und kann Daten auslesen oder erhält vollständigen Zugriff (Remote-Controll)
* **Wie verhindert man Attacke auf verwundbare Stellen der/des Software/Betriebssystems**
  + Serialisierte Objekte aus Unbekannten Quellen verbieten
  + Integritätsprüfungen bei den empfangenen Daten
  + Empfangenen Code bzw. Daten isolieren und in niedrigen Berechtigungsebenen ausführen. Beispiel Segmentierung durch Container
  + Prüfungen auf Ausnahmen und Fehler.
  + Typ der empfangenen Daten überprüfen. Wurde dieser Typ überhaupt erwartet oder war es ein Angriff?
  + Überwachung der Verbindung, wird die Leitung Blockiert? Löst die Deserialisierung ein unerwartetes Verhalten aus?
  + Abbruch der Verbindung wenn eine Übertragung nach einer gewissen Zeit nicht beendet wird.
* **Ziele eines Angreifers (Umgebung und Nutzen)**
  + Der Angreifer möchte Zugriff auf das Opfer System erhalten. Daten stehlen oder manipulieren und somit Schaden anrichten bzw. einen Nutzen zu ziehen.
  + Den Zugriff blockieren oder einschränken
  + Die Umgebungen welche Angegriffen werden, sind alle bei denen Daten übertragen, empfangen oder ausgetauscht werden
  + Anwendungen die einen Zustand speichern oder erhalten müssen
* **Gefährdete Personengruppen**
  + Jeder Nutzer der ein System mit Internetzugang besitzt und Daten empfängt