Name des Angriffs:

Unsichere Deserialisierungsfehler

Ziel des Angreifers:  
serialisiert Objekte an das Opfer senden um Schaden anzurichten, Leitungen zu blockieren oder Zugriff zu erhalten (Remote-Code-Ausführung).

Schutzmaßnahmen:

Serialisiert Objekte aus unbekannten Quellen verbieten.

Integritätsprüfung

Code isolieren und niedrigen Berechtigungseben ausführen

Auf Ausnahmen und Fehler prüfen: ist der Typ erwartet? Oder löst die Deserialisierung nicht erwartetes verhalten aus?

Konstante Überwachung der Verbindung. Wird durch die Deserialisierung der Verbindung beeinträchtigt?

Angriffszenarios:

Senden von Serialisierten Objekten

Gefährdete Personengruppen:

jeder der Daten die Serialisiert wurden um eine Übertragung zu erleichtern empfängt und diese dann Deserialisiert

Umgebung:

Alle Anwendungen die einen Zustand speichern oder erhalten müssen.

Anwendungen die Daten Empfangen oder eine Client-Server Architektur verwernden.

Merkmal:

Nicht bekannte neue Nutzer

Unbekannte Anfragen bei der Übertragung von Daten