AYI NEDJIMI Consultants

Désérialisation : Attaques Java, PH

30 April 2026 • Mis à jour le 30 April 2026 • 49 min de lecture

> Guide expert désérialisation : ysoserial Java, POP chains PHP, BinaryForm
> et défense complètes.

La **désérialisation insécurisée** (insecure deserialization) figure parmi les vulnérab
moderne, permettant l'exécution de code arbitraire à distance (RCE) sur des serve
préalable. Classée en position A08 dans l'**OWASP Top 10 2021** et identifiée comm
classe de vulnérabilités a été exploitée dans certaines des attaques les plus retent
massive d'Equifax via Apache Struts, les campagnes ciblant les serveurs **JBoss** et
Magento et **Laravel**, et plus récemment les exploitations de **ViewState** .NET dans
fondamental est redoutablement simple : lorsqu'une application reconstruit un obj
attaquant, celui-ci peut injecter des objets malveillants qui déclenchent des chaîne
de commandes système. L'outil **ysoserial** et ses variantes ont démocratisé l'explo
chains en PHP et les payloads **pickle** en Python ont élargi la surface d'attaque à l'
analyse en profondeur les mécanismes de désérialisation exploitable dans chaque
de détection avancées et les stratégies défensives pour neutraliser cette menace
bibliothèques et frameworks.

À RETENIR

Points clés de cet article :

La désérialisation insécurisée permet l'exécution de code arbitraire à distar PHP, .NET et Python

Les gadget chains sont des séquences de méthodes existantes dans le cla aboutissent à l'exécution de commandes

L'outil ysoserial automatise la génération de payloads exploitant les bibliotl CommonsBeanutils, Spring, etc.)

En PHP, la fonction `unserialize()` combinée aux magic methods (`__wak` vecteurs d'attaque POP chain

En .NET, `BinaryFormatter` , `ObjectStateFormatter` et les ViewState non

Le module Python `pickle` est intrinsèquement dangereux car il permet l'e

La défense repose sur l'abandon des formats de sérialisation natifs au prof d'allowlists de classes

Fondamentaux de la sérialisation et de la désérialisation

La sérialisation est le processus de conversion d'un objet en mémoire en un flux d stocké ou transmis, tandis que la désérialisation est l'opération inverse qui recons omniprésent dans les architectures logicielles modernes : sessions utilisateur, cac communication inter-services (RMI, RPC), API REST/SOAP et persistance d'état. C mécanismes natifs de sérialisation, chacun avec ses spécificités et ses risques de