What is insecure deserialization?

Insecure deserialization is a vulnerability where an application rebuilds (deserializes) objects from untrusted input without validating it, so an attacker crafts a serialized payload that executes code or alters application logic when it is loaded. Because deserialization can instantiate arbitrary objects and trigger their methods, it frequently leads to remote code execution through gadget chains. It is caused by trusting serialized data from users or cookies, and the fix is to avoid deserializing untrusted input or use safe, data-only formats.

HOW IT WORKS

01 How it works and example

The attacker supplies a malicious serialized object where the app expects a trusted one (a cookie, a hidden field, an API body, a cache entry):

- Java: a serialized object using a known gadget chain (tools like ysoserial generate these) to reach `Runtime.exec`.
- PHP: an `O:` serialized string crafted so a class's `__wakeup`/`__destruct` performs a dangerous action (PHP object injection).
- Python: a malicious pickle that runs code via `__reduce__` when loaded.
- .NET: gadget chains via `BinaryFormatter`.

The payload runs as the application loads it. Examples shown for defensive context.

> LOADING IS EXECUTING
>
> *The core lesson: with unsafe formats, deserializing data can execute code. Never feed untrusted bytes to a deserializer that can instantiate arbitrary objects (Java native serialization, Python pickle, PHP unserialize, .NET BinaryFormatter).*

HOW TO DEFEND

- Do not deserialize untrusted input with formats that can instantiate arbitrary objects (pickle, Java native serialization, PHP unserialize, BinaryFormatter).
- Use data-only formats like JSON with a strict schema, mapping to known types.
- Integrity-protect any serialized data you must round-trip to a client (sign it) so it cannot be tampered with.
- Restrict allowed classes (look-ahead deserialization / allow-lists) where the format supports it.
- Patch libraries and test endpoints that accept serialized objects.

SOURCES

[1] OWASP: Deserialization

[2] MITRE CWE-502: Deserialization of Untrusted Data

[3] OWASP Top 10

Test your application for insecure deserialization and 30+ other classes.

securelayer7.net/learn/application-security/insecure-deserialization

Open online