Contribution ID: **17** Type: **not specified**

Analyzing Prerequistes of known Deserializtion Vulnerabilities on Java Applications

Wednesday, 5 June 2024 09:30 (15 minutes)

Insecure deserialization is regarded as one of the OWASP Top 10 software vulnerabilities. While requiring somewhat complex exploitation prerequisites, the impact of exposing this type of vulnerability is severe, often leading directly to remote code execution. The attack model is based on self-executing methods, invoked during the native deserialiaztion process - so-called gadget chains. Within the Java programming language this mostly refers to the invocation of *readObject()*. Serializable classes may override this method to implement custom deserialization logic, and thereby call further seemingly harmless methods. In our presentation we show how an attacker can leverage this to construct a chain of method invocations leading to undesirable effects. Furthermore, we analyzed and show how deserialization vulnerabilities rely on gadgets contained in third party libraries, affect latest JDK and library versions, and how one can use this information to gain visibility on the issue and harden Java applications.

Length

15 minutes

Optional: Speaker / convener biography

Primary authors: BARTEL, Alexandre (Umeå University); KREYSSIG, Bruno (Umeå University)

Presenter: KREYSSIG, Bruno (Umeå University)

Session Classification: Talks and presentations

Track Classification: Talks and presentations