Contribution ID: **7** Type: **not specified**

An In-depth Study of Java Deserialization Exploits

Tuesday, 27 June 2023 13:00 (45 minutes)

Deserialization is a technique based on rebuilding instances of objects from a byte stream. It can open applications to attacks such as remote code execution (RCE) if the data to deserialize originates from an untrusted source. Deserialization vulnerabilities are so critical that they are in OWASP's list of top 10 security risks for web applications. This is mainly caused by unwise decisions made during the development process of applications and by flaws in their dependencies such as libraries. In this talk we dissect Java deserialization vulnerabilities and discuss the analysis of gadgets based on 19 publicly known exploits. We observe that the modification of one innocent-looking detail in a class –such as making it public –can already introduce a gadget. Furthermore, 37.5% of the gadgets are not patched, leaving them available for future attacks.

Have you presented this talk before

Yes

Talk length

45

Primary authors: BARTEL, Alexandre (Umeå University); Mr JANSSON, Glenn

Presenters: BARTEL, Alexandre (Umeå University); Mr JANSSON, Glenn

Session Classification: Talks

Track Classification: Talks