Automated detection of deserialization vulnerabilities in .NET applications

Mikhail Shcherbakov and Musard Balliu
KTH Royal Institute of Technology

Vulnerabilities in the process of data deserialization are known for more than 10 years. In the last few years, attacks against insecure deserialization have attracted a lot of attention. Many .NET and Java web applications are vulnerable to this kind of attack. Many new payloads have been discovered over the last couple years. The impact of deserialization flaws can lead to exploitation of remote code execution (RCE) attacks, one of the most dangerous attacks possible.

We study the code of serialization libraries in the context of .NET platform and identify formal patterns leading to this kind of attack. We also describe the threat model for web applications where insecure deserialization can serve as post-exploitation for other types of attacks and thus increase the impact on the attacked system. We study new approaches for control flow and data flow analyzes to statically detect the described patterns in the code. Furthermore, we present the first results of our prototype static analyzer for Common Intermediate Language (CIL) for finding vulnerabilities in real-world applications.