1400 - Friday the 13th: JSON attacks!

Sunday at 14:00 in Track 4
45 minutes | Demo, Exploit

Alvaro Muñoz*Principal Security Researcher,Hewlett Packard Enterprise*

Oleksandr Mirosh*Senior Security QA Engineer, Hewlett Packard Enterprise*

2016 was the year of Java deserialization apocalypse. Although Java Deserialization attacks were known for years, the publication of the Apache Commons Collection Remote Code Execution (RCE from now on) gadget finally brought this forgotten vulnerability to the spotlight and motivated the community to start finding and fixing these issues.

One of the most suggested solutions for avoiding Java deserialization issues was to move away from Java Deserialization altogether and use safer formats such as JSON. In this talk, we will analyze the most popular JSON parsers in both .NET and Java for potential RCE vectors.

We will demonstrate that RCE is also possible in these libraries and present details about the ones that are vulnerable to RCE by default. We will also discuss common configurations that make other libraries vulnerable.

In addition to focusing on JSON format, we will generalize the attack techniques to other serialization formats. In particular, we will pay close attention to several serialization formats in .NET. These formats have also been known to be vulnerable since 2012 but the lack of known RCE gadgets led some software vendors to not take this issue seriously. We hope this talk will change this. With the intention of bringing the due attention to this vulnerability class in .NET, we will review the known vulnerable formats, present other formats which we found to be vulnerable as well and conclude presenting several gadgets from system libraries that may be used to achieve RCE in a stable way: no memory corruption — just simple process invocation.

Finally, we will provide recommendations on how to determine if your code is vulnerable, provide remediation advice, and discuss alternative approaches.
Alvaro Muñoz
Alvaro Muñoz (@pwntester) works as Principal Software Security Researcher with HPE Security Fortify, Software Security Research (SSR). His research focuses on different programming languages and web application frameworks searching for vulnerabilities or unsafe uses of APIs. Before joining the research team, he worked as an Application Security Consultant

helping enterprises to deploy their application security programs. Muñoz has presented at many Security conferences including DEF CON , RSA, AppSecEU, Protect, DISCCON, etc and holds several infosec certifications, including OSCP, GWAPT and CISSP, and is a proud member of int3pids CTF team. He blogs at http://www.pwntester.com.

@pwntester
Oleksandr Mirosh
Oleksandr Mirosh has over 9 years of computer security experience, including vulnerability research, penetration testing, reverse engineering, fuzzing, developing exploits and consulting. He is working for HPE Software Security Research team investigating and analyzing new threats, vulnerabilities, security weaknesses, new techniques of exploiting security issues and development vulnerability detection, protection and remediation rules. In the past, he has performed a wide variety of security assessments, including design and code reviews, threat modelling, testing and fuzzing in order to identify and remove any existing or potentially emerging security defects in the software of various customers.

#defcon25/by_track/track4/sunday #defcon25/By_Day/_Sunday