j0lt-github / **jyaml Java library - 1.3 Deserialization attack**

Last active 2 years ago

jyaml Java library - 1.3 Deserialization attack

```
1  Description: JYaml through 1.3 allows remote code execution during deserialization of a malicious payload through the load() function. NOTE
2
3  VulnerabilityType: CWE-502: Deserialization of Untrusted Data
4
5  Vendor of Product: http://jyaml.sourceforge.net (see yaml.org)
6
7  Affected Product Code Base: jyaml Java library
8
9  Attack Type: Remote
10
11 Impact Code execution : True
12
13 Credits: Manmeet Singh and Ashish Kukreti
14
15 Attack Vectors : The jyaml can be exploited by deserialization of malicious YAML payload with default load() function of its object. The pa
16 https://github.com/mbechler/marshalsec
17 and passed to load function
18 like Object object = Yaml.load(new File("object.yml"));
19 it will certainly execute command.
20
21 Reference :
22 https://github.com/mbechler/marshalsec
23 https://github.com/mbechler/marshalsec/blob/master/marshalsec.pdf
24 https://sourceforge.net/p/jyaml/bugs/
25
26 Has vendor confirmed or acknowledged the vulnerability? : Yes
27
28 Discoverer : Manmeet Singh and Ashish Kukreti
```