

# [漏洞预警]泛微e-cology OA Beanshell组件远程代码执行分析

清水川崎 亚信安全网络攻防实验室 6天前

## 漏洞描述

泛微e-cology OA系统由于某些功能引用BeanShell.jar开发,但BeanShell组件且开放未授权访问,攻击者调用BeanShell组件接口可直接在目标服务器上执行任意命令.目前漏洞的安全补丁已由泛微官方发布,可参阅文末.

## CVE编号

暂无

## 漏洞威胁等级

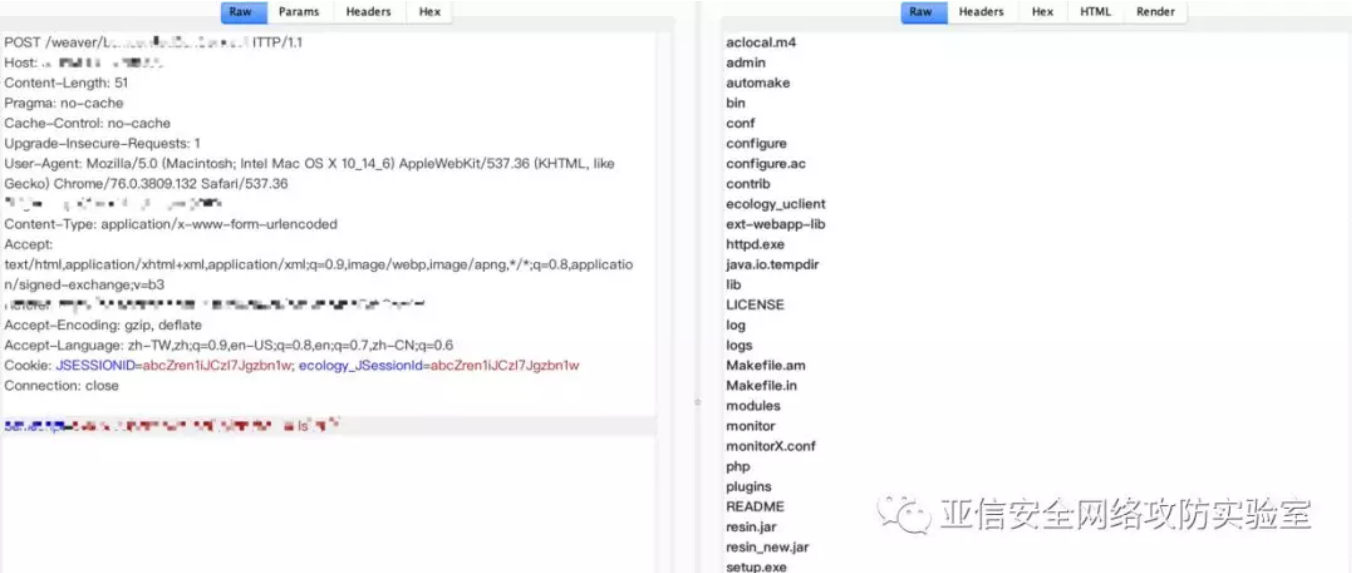
高危

## 影响范围

包括不限于7.0,8.0,8.1

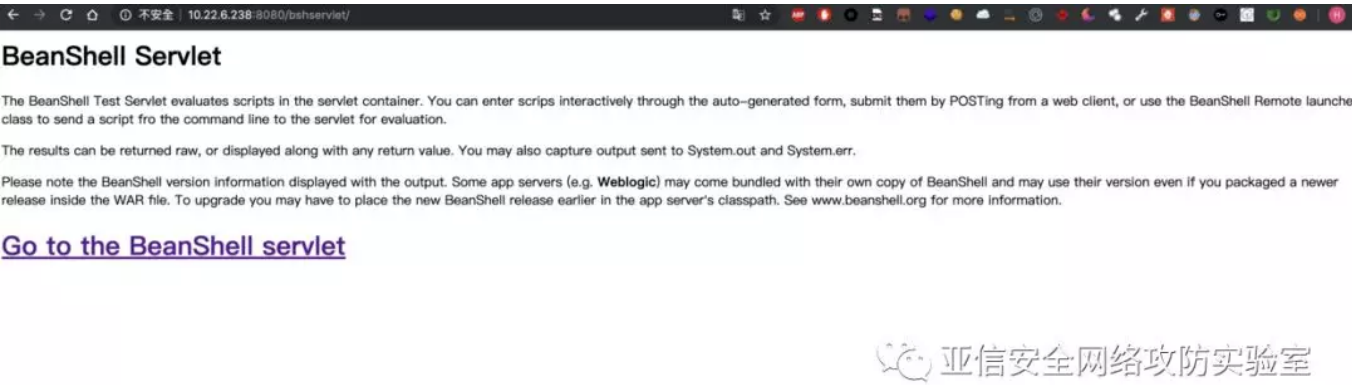
## 漏洞复现

使用payload进行验证



# 简单分析

由于此次存在漏洞的jar是Beanshell,于是我研究了一下Beanshel.  
参阅官方文档,下载了war包在本地搭建



# BeanShell Test Servlet

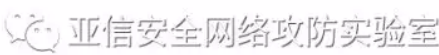
BeanShell version: 2.0b4

## Script

```
print("hello!");
```

Capture Stdout/Stderr: ☐ Display Raw Output: ☐

Evaluate



根据官方文档说明,我直接执行一个os命令,得到了回显

```
// Do a loop
for (i=0; i<5; i++)
    print(i);

// Pop up a frame with a button in it
button = new JButton( "My Button" );
frame = new JFrame( "My Frame" );
frame.getContentPane().add( button, "Center" );
frame.pack();
frame.setVisible(true);
```

## Useful BeanShell Commands

In the previous example we used a convenient "built-in" BeanShell command called `print()`, to display values. `print()` does pretty much the same as the command line. `print()` also displays some types of objects (such as arrays) more verbosely than Java would. Another related command is `toString()`.

Here are a few other examples of BeanShell commands:

- **source()**, **run()** – Read a bsh script into this interpreter, or run it in a new interpreter
- **frame()** – Display a GUI component in a Frame or JFrame.
- **load()**, **save()** – Load or save serializable objects to a file.
- **cd()**, **cat()**, **dir()**, **pwd()**, etc. – Unix-like shell commands
- **exec()** – Run a native application
- **javap()** – Print the methods and fields of an object, similar to the output of the Java `javap` command.
- **setAccessibility()** – Turn on unrestricted access to private and protected components.

See the complete list of [BeanShell Commands](#) for more information.

### Tip:

BeanShell commands are not really "built-in" but are simply BeanShell scripts that are automatically loaded into the classpath.

← → ↺ ⬆ ⓘ 不安全 | 10.22.6.238:8080/bshservlet/eval

# BeanShell Test Servlet

BeanShell version: 2.0b4

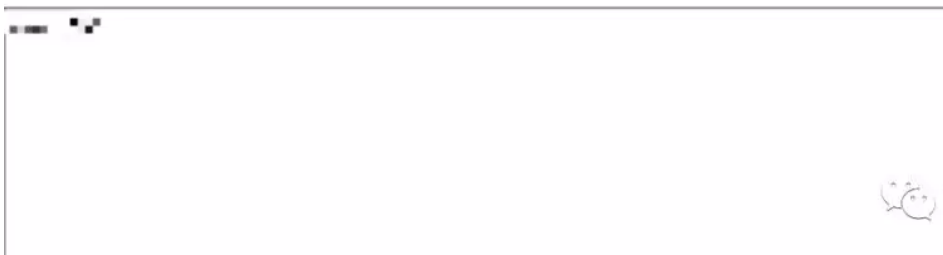
## Script Output

```
bootstrap.jar
catalina-tasks.xml
catalina.bat
catalina.sh
commons-daemon-native.tar.gz
commons-daemon.jar
configtest.bat
configtest.sh
daemon.sh
digest.bat
digest.sh
setclasspath.bat
setclasspath.sh
shutdown.bat
shutdown.sh
startup.bat
startup.sh
tomcat-juli.jar
tomcat-native.tar.gz
tool-wrapper.bat
tool-wrapper.sh
version.bat
version.sh
```

## Script Return Value

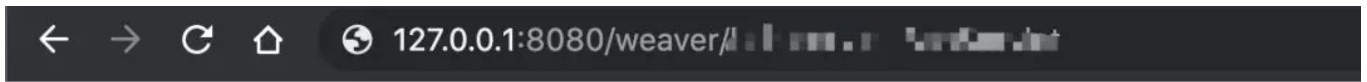
null

## Script



亚信安全网络攻防实验室

接着我到泛微e-cology OA环境下复现



# BeanShell Test Servlet

BeanShell version: 2.0b4

## Script Output

```
nt authority\system
```

## Script Return Value

null

## Script



Capture Stdout/Stderr: ☐ Display Raw Output: ☐

Evaluate

亚信安全网络攻防实验室

发现也成功了,但部分版本未成功,因为其做了全局函数过滤,需要绕过

```

Raw Params Headers Hex
POST /weaver/* HTTP/1.1
Host: ...
Content-Length: 26
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: ...
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6
Cookie: JSESSIONID=abcZren1jCzi7Jgzbn1w; ecology_JSessionId=abcZren1jCzi7Jgzbn1w
Connection: close

bsh.script=...

```

```

Raw Headers Hex Render
HTTP/1.1 200 OK
Server: Resin/3.1.8
Content-Type: text/html; charset=utf-8
Connection: close
Date: Fri, 20 Sep 2019 06:33:43 GMT
Content-Length: 148

<script
language="javascript">try{top.Dialog.alert("提示:系统错误.");}catch(e){alert("提示:系统错误.");}window.history.go(-1);</script>

```

亚信安全网络攻防实验室

随后在朋友的帮助下,成功绕过了过滤

```

Raw Params Headers Hex
POST /weaver/* HTTP/1.1
Host: ...
Content-Length: 51
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: ...
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6
Cookie: JSESSIONID=abcZren1jCzi7Jgzbn1w; ecology_JSessionId=abcZren1jCzi7Jgzbn1w
Connection: close

...

```

```

Raw Headers Hex HTML Render
aclocal.m4
admin
automake
bin
conf
configure
configure.ac
contrib
ecology_uclient
ext-webapp-lib
httpd.exe
java.io.tmpdir
lib
LICENSE
log
logs
Makefile.am
Makefile.in
modules
monitor
monitorX.conf
php
plugins
README
resin.jar
resin_new.jar
setup.exe

```

亚信安全网络攻防实验室

鸣谢(排名不分先后)

pyn3rd

thesoul(404)

lufei

## Reference

Beanshell官方指南:

<https://beanshell.github.io/>

补丁包下载:

<https://www.weaver.com.cn/cs/securityDownload.asp>