I4-2IDocView-在线文档解析应用-任意文件读取

漏洞描述:

iDocView是一个在线文档预览系统/doc/upload 接口处存在任意<u>文件读取</u>漏洞,未授权的攻击者可以利用此接口并携带默认token读取服务器敏感文件信息,使系统处于极度不安全的状态。

网站图片:

I Doc View

在线文档预览、压缩文件预览、图纸预览、图片预协作编辑、同步展示等 - I Doc View

文档类: doc, docx, xls, xlsx, ppt, pptx, pdf, txt

图片类: jpg, gif, png, bmp, tif 音频类: mp3, m4a, midi, wma 压缩文件类: zip, rar, tar, 7z 图纸类: dwg, dxf, dwf

Version: 7.3.11_20170502

网络测绘:

fofa语法:

FOFA: title=""在线文档预览 - I Doc View"

漏洞复现:

payload:

效果图:

{"ext":"txt","code":"1","size":"167","name":"time.txt","nname":"test.txt","srcUrl": //data/test/2023/1031/15/151534_167_OCHiYvt.txt", rid":"test_

PS: 访问srcUrl返回路径,即可读取文件内容

← → C ▲ 不安全 こここここ5:8083/data/test/2023/1031/15/151534_167_OCHiYvt.txt

for 16-bit app support [fonts]

[extensions] [mci extensions]

[files] [Mail]

MAPT=1

CMCDLLNAME32=mapi32.d11

CMC=1 MAPTX=1

MAPIXVER=1.0.0.1