1、前言

用友GRP-U8 R10行政事业财务管理软件是用友公司专注于电子政务事业，基于云计
算技
术所推出
的新一代产品，是
我国行政事业财务领域专业的财务管
理软件。
近日，百度云安全团队监测到有研
究人员披露了用友GRP-U8任意SQL语句执行漏洞的POC，并可利用SQL SERVER数据库特性执行系统命令，我们对漏洞进行了复现和分析，发现该漏洞危害严重，请广大用户及时进行升级修复。

2、环境搭建

通过搜索发现用友GRP-U8存在3个版本，分别为B版、C版、G版，其中B版，C版和G版模块数量、结构不一样，B版和C版是CS结构，G版可以用浏览器登录。我们需要下载G版进行安装。

安装完成后，目录结构如下，其中webserver为tomcat目录，webapps为Web目录。

跟进到com.anyi.midas.MidasProxy，POST请求进入doPost方法，并随后调用了Dispatcher的Process方法处理请求。

进入processRequestInfo方法，73行获取请求中ec参数，当ec为空时，加密选项为false；因此，为了方便编写POC，ec参数需要置空，97行调用XMLTools类将dp参数中的xml内容进行解析，方便后续直接获取xml内容中各个参数的值。

跟进看看as_DataRequest方法是如何定义的，其中参数providerName来自XML的PARAM标签下ProviderName标签的值，参数data则为Data标签的值，均为外部可控值。64行调用了ProviderFactory类的getProvider方法。

跟进到QueryProvider类的dataRequest方法，该方法调用了DBTools类的executeSQL方法。

跟进到executeQueryAction_Buffer方法，199行判断数据库是否为oracle，GRP-U8默认为SQL SERVER数据库，因此进入else语句后，206行通过stmt对象调用了executeQuery方法执行了可控的sql参数，并且整个过程中没有SQL语句拼接，可导致任意SQL语句执行。