

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。

```
728 </servlet>
729 <servlet-name>Proxy</servlet-name>
730 <servlet-class>com.anyi.midas.MidasProxy</servlet-class>
731 </servlet>
732 <servlet-mapping>
733 <servlet-name>Proxy</servlet-name>
734 <servlet-class>com.anyi.midas.MidasProxy</servlet-class>
735 </servlet-mapping>
736 </servlets>
737 <servlet-name>Todo</servlet-name>
738 <servlet-class>com.uf.gov.midas.pt.TodoProxy</servlet-class>
739 </servlet>
```

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。

```
28 public static void Process(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException {
29     RequestInfo rqi = new RequestInfo(request);
30
31     try {
32         String errStr;
33         ErrorCodes ec;
34         ServletOutputStream stream;
35         try {
36             rqi.testTime = StringTools.outputTime("in process request");
37             rqi.processRequestInfo(request);
```

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d p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。

```
28 if (rqi.getFunctionName().equalsIgnoreCase("AS_GetDataReq")) {
29     return;
30 }
31
32 if (rqi.getFunctionName().equalsIgnoreCase("AS_LeaveSession")) {
33     DataModule.as_EnterSession(rqi, rqi.getProviderName());
34     rqi.setResultXML(new ResultPacket(new Data(new Variant(""))).toXML(rqi.httpSessionId));
35     response.setContentType("text/html; charset=UTF-8");
36     response.getWriter().write(rqi.getResultXML());
37     rqi.testTime = StringTools.outputTime("in process request " + rqi.getFunctionName() + " 线程ID: " + rqi.threadId);
38 } else if (rqi.getFunctionName().equalsIgnoreCase("AS_LeaveSession")) {
39     rqi.testTime = StringTools.outputTime("in process request " + rqi.getFunctionName() + " 线程ID: " + rqi.threadId);
40     DataModule.as_LeaveSession(rqi, rqi.getProviderName());
41     rqi.setResultXML(new ResultPacket(new Data(new Variant(""))).toXML(rqi.httpSessionId));
42     response.setContentType("text/html; charset=UTF-8");
```

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。

```
11 |
12 |
13 | public static Provider getProvider(String providerName) {
14 |     if (providerName.equalsIgnoreCase("QueryProvider")) {
15 |         return new QueryProvider();
16 |     } else if (providerName.equalsIgnoreCase("DataSetProviderExec") {
17 |         return new UpdateProvider();
18 |     } else if (providerName.equalsIgnoreCase("SQLProvider") {
19 |         return new SQLProvider();
20 |     } else if (providerName.equalsIgnoreCase("AppUpdateProvider") {
21 |         return new DataProvider();
22 |     } else if (providerName.equalsIgnoreCase("ReadmapProvider")) {
23 |         return new RSPProvider();
24 |     } else {
25 |         return (Provider)(providerName.equalsIgnoreCase("OracleProvider") ? new RSPProvider() : new SQLProvider());
26 |     }
27 | }
28 |
```

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

```
140 public static void executeSQL_Buffer(RequestInfo rqi, String sql, String sqlType) throws BusinessException
141     if (!sql.equalsIgnoreCase("ClearSQL") && !sql.equalsIgnoreCase("EXECSQL")) {
142         Statement stmt = null;
143     }
144     try {
145         stmt = rqi.connection.createStatement();
146         if (sqlType.equalsIgnoreCase("query")) {
147             executeQueryAction_Buffer(rqi, stmt, sql);
148         } else if (sqlType.equalsIgnoreCase("insertquery")) {
149             executeAction_Buffer(rqi, stmt, sql);
150         } else if (isNoDataSql(sql)) {
151             executeAction_Buffer(rqi, stmt, sql);
152         } else if (isUpdateSql(sql)) {
153             executeAction_Buffer(rqi, stmt, sql);
154         }
155     } catch (SQLException e) {
156         // ...
157     }
158 }
```

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。

