QT系统集成组 - Bug #2941

SHL06CIOS的 FEP2.1协议 cctvC3jt导致 fepdaq主程序崩溃

04/12/2023 11:18 AM - yufeng wu

Status:	Resolved	**Start date:**	04/10/2023
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

20230408电科王赛报 C3 6号线FEPwin2.1崩溃，弹出崩溃出错窗关联协议库cctvC3jt.dll
SHL06CIOSfep21cctvC3jt崩溃_20230408.jpg
代码发现收到cctv消息message字串超过100长度后，会导致print %s 打印字串缓存延伸超长

```
141     /*infotype=1按键，2平台回复*/
142     /*keyvalue=0-9数字，10方向停止，11-18上下左右-左上-左下-右上-右下（步长0-8），20-21变倍大小，22-23近远，24-25光圈大小，
143     26DEVC,27CAM,28MON,29TOUR,30MAC,31PATTERN,32AUTOPAN,33GOTO,34ENTER,35MULT,36WIN,37CAN-G,38MON-G,39GROUP,40SET,41PT,42LOCK,43SHIFT,44ESC
144     45跳页，46上一页，47下一页，48轮巡开始，49轮巡停止，50轮巡暂停*/
145     /*platinfotype=1选择消息回复：2轮巡回复：3云台：4报警：5回显：6状态信息（Mon、Win通道、Cam）     */
146     keylen=12;
147     ctmp=NULL;memset(cVal,0,16);
148     if(NULL!=(ctmp=GetAkeyVal(tmp,"platinfotype",keylen)))
149     {
150         memcpy(cVal,ctmp,keylen);
151         m_platinfotype=atoi(cVal);
152         PrintLog(LOG_INFORMATION,"platinfotype=%s     ", cVal);
153     }
154     keylen=7;
155     ctmp=NULL;memset(cVal,0,16);
156     if(NULL!=(ctmp=GetAkeyVal(tmp,"message",keylen)))
157     {   memset(m_msg,0,100);
158         memcpy(m_msg,ctmp,keylen);
159         PrintLog(LOG_INFORMATION,"message=%s     ", cVal);
160     }
161     keylen=3;
162     ctmp=NULL;memset(cVal,0,16);
163     if(NULL!=(ctmp=GetAkeyVal(tmp,"Mon",keylen)))
164     {
165         memcpy(cVal,ctmp,keylen);
166         m_mon=atoi(cVal);
167         PrintLog(LOG_INFORMATION,"Mon=%s     ", cVal);
168     }
169     keylen=3;
170     ctmp=NULL;memset(cVal,0,16);
171     if(NULL!=(ctmp=GetAkeyVal(tmp,"Win",keylen)))
172     {
173         memcpy(cVal,ctmp,keylen);
174         m_win=atoi(cVal);
175         PrintLog(LOG_INFORMATION,"Win=%s     ", cVal);
176     }
177     keylen=3;
178     ctmp=NULL;memset(cVal,0,16);
179     if(NULL!=(ctmp=GetAkeyVal(tmp,"Cam",keylen)))
180     {
```

这里若keylen大于100时，也就是meeage字段的内容大于100个时，会把100之后的内容覆盖到内存地址在m_msg之后的变量中

结合头文件中关于m_msg的定义：
char m_msg[100];
int m_mon;
int m_win;
int m_cam;
uint8 m_mult;
char name[24];
char pwd[24];等等
若keylen大于113将影响name，keylen足够大时会把登录组包的buf[256]给撑爆

实际程序获取message字段的内容在m_msg中，这里用cVal的话会使每次打印日志都为空

CIOS6+CIOS5+CIOS7的竞天cctv键盘版本均有此问题

版本FEP win 2.1环境（VC++6编译环境）

History

#1 - 08/02/2023 09:19 AM - yufeng wu

- Status changed from New to Resolved

6-8号线换乘车站东体cctv改造，原接口内收到非法字串值 %s打印导致 溢出

Files

SHL06CIOSfep21cctvC3jt崩溃_20230408.jpg	450 KB	04/12/2023	yufeng wu
message超100字符会导致_s打印.png	145 KB	04/12/2023	yufeng wu