SUPER－WPS二例死机故障的原因分析及排除*

张 军
(盐城工学院学生处,盐城,224003)

摘 要 对SUPER－WPS系统在使用过程中最常见的二例死机故障的原因进行分析,并提出解决问题的具体措施和方法。

关键词 缓冲区 溢出 程序段 替代
分类号 TP36

目前,微机文字处理系统名目繁多,诸多微机用户由老版本的WPS移情基于WINDOWS的WORD或WPS97,但由于资金或技术等因素限制,仍有很大一部分用户使用着SUPER－WPS。WPS(2.X版)以占用微机资源小,简单实用的设计风格,曾使千百万用户为之倾倒,现在仍为初学者和一般文字处理用户所青睐。但是,SUPER－WPS还存在着设计缺陷,致使用户在使用中常会遇到这样或那样的问题,给用户带来不可挽回的损失。这些问题,有些是属于功能方面的,如对高版本DOS的兼容性问题、内存使用溢出问题等,另一类问题是由于设计缺陷造成的软件故障,这些故障具有严重的破坏性,常给使用者造成重大损失,死机故障是最常见的一种。在用WPS编辑文稿时,或在编辑模式调用WPS某一功能时,常会出现死机现象,从而使使用者做的工作付之东流。本文列举二例较为常见的故障现象,作一简单的讨论。

1 死机故障之一

常见的一种死机故障出现在做删除操作的时候。WPS为删除操作(块删除除外)开辟了一个225字节长的缓冲区,用于暂存被删除的内容,使使用者可能恢复刚删除的内容。做删除时死机,是这个缓冲区溢出造成的。WPS一次可以编辑不大于60KB的文件,当文件的长度大于60KB时,WPS将取其中大于60KB的部分进行编辑。当在被编辑部分的底部做删除操作时,如果正好删除最后一行或最后一个字符,WPS将启动读磁盘操作,读取文件的后续部分,以保持屏幕显示的完整。此时,WPS对缓冲字计数的计算发生溢出错误,造成数据缓冲时缓冲区严重溢出,数据覆盖程序执行代码段,造成死机。

用程序1替代WPS.EXE中相应的代码段,可以消除这一故障。修改可使用DEBUG进行,先将WPS.EXE改名为非EXE文件,DEBUG装入后,用程序段1替代原程序51ABH～51DAH的程序段。

程序1:

收稿日期:1998－02－16

```
51AB PUSH AX
52AC  CALL  8CF7
51AF  XCHG  SI,[02A2]
51B3  CALL  8DD2
51B6  MOV  CX,SI
51B8  MOV  SI,[02A2]
51BC  SUB  CX,SI
51BE  JBE  51D1
51C0  MOV BYTE  PTR[0093],01
51C5  DEC  WORD  PTR[0094]
51C9  PUSH  CX
51CA  CALL 8628
51CD  POP  CX
51CE  CALL 9166
51D1  POP AX
51D2  CMP  [02B5],AX
51D6  JZ  51E0
51D8  MOV  [02B5],AX
```

2　死机故障之二

WPS具有开窗口和DOS　SHELL的功能，但在调用这两个功能时常会莫名其妙地死机。其实，这种现象只在模拟显示或调用打印功能后，再调用上述功能时才会出现。为避免造成不必要的损失，在模拟显示或打印文件之后，不能调用开窗口和DOS　SHELL功能，或在调用这些功能之前先保存文件。值得注意的是，在模拟显示或打印之后，卸掉CCDOS，再重新安装，调用开窗口和DOS　SHELL功能同样会死机。说明出现这一故障的原因不在WPS本身，而在CCDOS。

金山CCDOS5.1版具有EMS管理功能，使用中断号67H。它有四个基本功能调用，即分配扩展内存，释放扩展内存，送数据块到扩展内存，从扩展内存读数据块。用户可以通过EMS功能调用，以64KB为块，申请多达4MB扩展内存。这些功能的具体用法可参见WPS用户手册。WPS在模拟显示和打印文件时，调用了EMS功能，开窗口和DOS　SHELL功能也要调用EMS，以保存现场数据。死机故障是EMS错误分配和释放扩展内存造成的。在分配和释放扩展内存时，EMS没有对某些特定的条件进行检查，以致于原来并未分配的内存被“释放”，而已分配的扩展内存却被“再分配”，后果就可想而知了。解决的办法就是为EMS增加特定条件的检查，具体来讲就是：

①在SPDOS.COM的地址1127H处指令SUB　AX,[1072]之后，增加一条JBE　××××指令。

②在SP DOS.COM的地址118BH处指令XOR　BX,BX之后，插入指令OR AX,AX，JZ××××。

CCDOS的EMS程序段编写得比较紧凑，增加指令需要对程序段作一些调整。读者可用程序2替代SPDOS.COM的10FEH到118CH之间的代码段。替代完成后，还须将10F6H处的值改为1BH，将10F8H处的值改为81H。这样改完以后，EMS就可以正常工作了。

程序2：

```
10FE  PUSHA
10FF  PUSH  DS
1100  PUSH  ES
1101  PUSH  CS
1102  PUSH  CS
1103  POP  DS
1104  POP  ES
1105  CMP  AH,04
1108  JNB  1118
110A  MOV  DX,BX
110C  MOV  BL,AH
110E  XOR  BH,BH
1110  SHL  BX,1
1112  XOR  AH,AH
1114  JMP  [BX+10F6]
1118  JMP  11A1
111B  AL,40
111D  MUL DL
```

```
111F MOV DX,AX
1121 MOV AX,[1070]
1124 SUB AX,[1072]
1128 MOV BX,DX
112A JBE 1130
112C CMP AX,DX
112E JNB 1132
1130 JMP 1167
1132 MOV SI,1076
1135 MOV AX,0001
1138 CMP WORD PTR[SI],+00
113B JZ 1143
113D ADD SI,+02
1140 INC AX
1141 JMP 1138
1143 MOV[SI],AX
1145 ADD SI,+02
1148 SUB DX,+40
114B JB 116E
114D JZ 116E
114F CMP WORD PTR[SI]+00
1152 JZ 1143
1154 MOV SI,1076
1157 MOV CX,0040
115A CMP [SI],AX
115C JNZ 1162
115E MOV WORD PTR[SI],0000
1162 ADD SI,+02
1165 LOOP 115A
1167 POP ES
1168 POP DS
1169 STC
116A POPA
116B RETF 0002
116E ADD[1072],BX
1172 MOV[1074],AX
1175 POP ES
1176 POP DS
1177 POP A
1178 CS:
1179 MOV AX,[1074]
117C CLC
117D RETF 0002
1180 NOP
1181 MOV SI,1076
1184 MOV CX,0040
1187 XOR BX,BX
1189 OR AX,AX
118B JZ 1167
```

以上程序1、程序2均在COMPAQ386－33、兼容486－66机型中测试通过。

参 考 文 献

1 赵明渊. 微机应用与软件开发. 四川科学技术出版社. 1993
2 章国英. 计算机软件出错信息大全. 同济大学出版社. 1995

Analyses & Solutions to Two Cases of Halt in Super - wps system

Zhang Jun
(Student Department of Yancheng Institute of technology, Yancheng, 224003, PRC)

Abstract The author analyses the reasons to two common cases of halt in the use of super - wps system and recommends solutions to them.

Keywords buffer; overflow; program segment; replace