

解除CCED的日期限制

TP31

广东省物价局 刘 川

在 CCED.EXE 和辅助程序 DBST.EXE 中(Ver 02-24-1989,文件长度分别为 86930 和 41884 字节),均设置有系统日期检测过程作为程序使用寿命的限制,当系统日期年份 < 1992 年时可以进入正常的操作;当系统日期年份 > 1992 年时,则只是显示标题和“CCED 使用期限已到,需要更新版本”的信息之后退出,使程序无法继续使用。

程序获取系统日期是由 DOS INT 21H 中断的 2AH 号子功能完成的,调用的汇编语句为 MOV AH,2A INT21,程序代码为 B42A CD21,返回结果年份在 CX。由于程序只作年份值检查而不检查月日值,故要解除 CCED 的日期限制,只需取消程序读系统日期的操作,代之以设置 CX 为 CCED 认可的年份值(例如 1991 年),使程序认为“读”到的年份为合法值而可以进入程序的正常操作,从而可解除 CCED 对日期的限制。使用 PCTools 可以非常方便地完成这项修改。

首先用 PCTools 的 Find 功能查出代码 B42ACD21 在 CCED.EXE 中的偏移位置,显示结果为:

```
search argument found in relative sector 00149
offset 0044
```

```
press "E" to view / edit the sector or
"G" to continue searching
```

相当于在程序的第 76332 字节处。此时按 E 键可以直接进入 FILE View / Edit 状态,屏幕显示 CCED.EXE 的代码内容,并且光标停在相对扇区 149 偏移 44 字处。可见到下面几个字节:

```
50 51 52 56 BB 0A 00 E8 C1 06 53 52 B4 2A CD 21
```

将它们修改成:

```
50 51 52 56 BB 0A 00 E8 C1 06 53 52 B9 C7 07 90
```

在光标所在位置起可以看到代码 B42ACD21,如图中的下划线部分。这时可以将这四个字节修改为 B9C70790(汇编语句为 MOV CX,07C7,设置 CX = 1991 年,剩下一个字节用空操作码 90H 填充),按 F5 键将修改结果存盘,然后结束修改,退出 PCTools,完成对程序的修改工作。这时 CCED.EXE 已解除了对日期的限制,无论系统日期为哪一年份都可以正常使用。

对 CCED 的辅助程序 DBST.EXE 的修改方法与对 CCED.EXE 的修改方法完全相似。用 PCTools 的 Find 功能可以查出代码 B42AD21 在程序中的偏移位置为相对扇区 0063 偏移 281 字节,相当于在程序的第 32537 字节处。用同样的方法将这四个字节修改为 B9C70790 然后存盘退出即可完成对辅助程序 DBST.EXE 的修改。

由于 DBST.EXE 的默认打表日期是取系统日期,并且与检测程序使用期限调用同一过程来获取系统日期,而此时程序中原来读系统日期过程已被修改因而无法返回正确的系统日期参数,返回的结果只是一个固定的年份值 CX = 07C7H,在 DX 中的月、日值未知,已没有意义。因此,在使用修改后的 DBST.EXE 时需要注意,建立参数表文件 DBST 时必须指定打表日期的年、月、日而不能使用默认参数--使用系统日期,出就是在 DBST 文件中必须有 /Y = XXXX /M = XX /D = XX 参数指定年月日。

164