

DMS100 用户公告

编号: CAB.PRC.7006

Customer Advisory Bulletin

发布日期: 2007/06/20 状态: A

有效范围: 全国

设备类型: DMS100I

适用版本: DMS100 所有 BCS 版本

问题级别 (一般、重要、紧急): 重要

撰写人: Arthur Pan

(CHINA ETAS, GDNT)

标题: 使用自定义命令避免 TRAP 的建议

问题描述:

在北电DMS100i交换机系统中, 通过使用自定义命令可以简化输入, 提高维护效率。但是不规范的自定义命令在使用过程中会导致TRAP产生。如下所示: 给用户线添加叫醒服务功能(WUC)时, 自定义的命令也是WUC, 该命令在servord 层下使用不会出现问题。一旦用户退出 servord 层, 在CI层执行命令, 就会产生TRAP.

示例如下:

```
CI:
>command wuc (ado $ @1 wuc $ y y)
>
2007/05/25 17:23 <<*>> LD156261 CHINA RBCS45BN SN60 IS NODATA Feb.10
Netas <<*>>
CI:
>wuc
Trap 12. PROCID: #2511 #50B0: dead trapped
at 042F1918=CI.FM06:EXAMINET+#001C.
Stack overflow.
2007/05/25 17:23 <<*>> LD156261 CHINA RBCS45BN SN60 IS NODATA Feb.10
Netas <<*>>
```

产生 TRAP 报告如下:

```
GUWACIBJDS0 TRAP MAY09 13:08:47 6400
Trap number 1783, Stack overflow.
```

```
At 042F1918=CI.FM06:EXAMINET+#001C,  
PROCID= #2511 #3078: dead, Entry Module: CIPROC SSTI: #01B2  
Current count of this trap type: 74  
Traceback:  
    B3DD7FD0 (Procname Unknown)
```

HARDWARE REGISTERS:

TIC Configuration Register	0202 0002
TIC Set Interrupt Level Register	0808 0008
TIC Interrupt Register	0000 0000
TIC Interrupt Cause Register	0000 0800
TIC Secondary Interrupt Register	0000 8000
TIC General Interrupt Mask	0001 00AB
MEI Configuration Register	00C0 E1F4
MEI LMS Write Protect Override	0000 0000
MEI E CORE Error AHR	2041 0050
MEI General Fault Register	0000 0000
PCCAB Control Register	0000 0000
PCCAB Status Register	0000 0000
PCCAB ECC AHR	0000 0000
PFAR	B3DD 7FD0
PFSR	0005 0000
Primary Maintenance AHR	B3DD 7FD0
FIR	No bits set in FIR.

TRAP in SYNC.

*** PLEASE CAPTURE FULL TRAPINFO FOR DEBUGGING ***

问题分析:

在上述的例子中, 根据定义, 系统在执行WUC时, 对命令解析为:

```
> ado $ @1 wuc $ y y
```

如果当前是在servord层下执行, ADO 是可以识别的命令, ADO 以后的数据将根据ADO命令的格式进行处理, 在这种情况下WUC作为系统定义的叫醒服务的名字, 赋给ADO命令。命令正常执行。

但是, 如果用户在CI层执行命令, 系统解析时, ADO 不可识别。系统继续搜索解析以后的字符串, 当搜索到WUC时, 发现此命令可以执行。于是WUC再次被当作我们定义的命令进行解析处理, 这样, 对命令WUC的解析产生了死循环。内存堆栈溢出, 产生TRAP。

这种情况类似使用如下自定义:

```
>command abc (abc)
>
2007/05/18 22:48 ***BCS45_070608, IDTC 0 --> IDTC 1, PLGC 2 --> PLGC 1***
CI:
>abc
Trap 9. PROCID: #2510 #1045: dead trapped
at 042F1918=CI.FM06:EXAMINET+#001C.
Stack overflow.
2007/05/18 22:48 ***BCS45_070608, IDTC 0 --> IDTC 1, PLGC 2 --> PLGC 1***
>
```

另外, 如果我们已经错误地定义了一个命令, 在以后我们再次调用到这个命令时, 同样也会出 TRAP: 例如:

```
2007/05/18 22:48 ***BCS45_070608, IDTC 0 --> IDTC 1, PLGC 2 --> PLGC 1***
CI:
>command wuc (ado $ @1 wuc $ y y n)
2007/05/18 22:48 ***BCS45_070608, IDTC 0 --> IDTC 1, PLGC 2 --> PLGC 1***
CI:
>command www (ado $ @1 wuc $ y y n)
2007/05/18 22:48 ***BCS45_070608, IDTC 0 --> IDTC 1, PLGC 2 --> PLGC 1***
CI:
>www
Trap 2. PROCID: #2510 #20C8: dead trapped
at 042F1918=CI.FM06:EXAMINET+#001C.
Stack overflow.
2007/05/18 22:48 ***BCS45_070608, IDTC 0 --> IDTC 1, PLGC 2 --> PLGC 1***
```

在上述例子中, 定义WWW给用户加WUC功能。但是, 如果在执行WWW之前, WUC已经错误地定义为给用户加WUC的命令。导致了WWW 命令调用了WUC命令, 按WUC命令执行解析时, 产生 TRAP。

处理建议:

广东北电正在开发补丁修正这个软件缺陷, 同时为避免问题的产生, 建议局方注意如下两点:

1. 建议局方在自定义命令时, 命令的内容不要出现该命令的字符串。否则非常容易出现命令解析的死循环, 导致堆栈溢出, 产生 TRAP。

例如:

避免使用如下命令进行定义:

COMMAND WUC (ADO \$ @1 WUC \$ Y Y)

可以用如下定义:

COMMAND WWW (ADO \$ @1 WUC \$ Y Y)

2. 清除以前定义的命令, 消除隐患。采用的方法有两种:
 1. 将用户 logout 再 login。彻底清除该用户自定义的命令。
 2. 用清除命令进行删除: >erase <命令名>

撤消

本通告不予撤消。