[TD 2696-CR] Application Problems after Patch Install and V4.0F/V5.0 - BLITZ

Unique Id: 009DD99D-E4746860-1C02A1

SOURCE: Compaq Computer Corporation INFORMATION BLITZ

INFORMATION BLITZ TITLE:

Possible problems with some applications, after installing the V4.0D/E BL 12 patch kit and V4.0F/V5.0 SSB.

DATE: 3-Sep-1999
INFORMATION BLITZ #: TD 2696-CR

AUTHOR: Henry Bone
TEL#: (603)884-6288
EMAIL: Henry.Bone@Compaq.com
DEPARTMENT: UNIX BUSINESS SEGMENT

==========

PRODUCT NAME(S) IMPACTED: Tru64 UNIX

PRODUCT FAMILY(IES):		PRODUCT NUMBERS:
Storage	___	_____
Systems	_x__	_Alpha_____
Networks	___	_____
PC	___	_____
Software	_x__	_V4.0D-F/V5.0___
Other (specify)	___	_____

PROBLEM STATEMENT:

The malloc() function in libc.so and libc.a has been updated. This version is distributed in the V4.0D/E BL12 patch kit, and V4.0F/V5.0 SSB. The new malloc() returns non-zeroed memory. This behavior remains consistent with all applicable standards, and is how malloc should be expected to work in the general case.

However, the older malloc() usually happened to return zeroed memory for malloc's of less than 632 bytes when the free() function had not yet been called by the process. Now it will usually leave non-zero data in the second longword of the allocated buffer. A few applications have proven to be sensitive to this change.

PROBLEM SYMPTOM:

When the application produces a string, an error message similar to the following will be seen:

```
save: SYSTEM error, 'service1M-PqM-Am-^?^C' is not a registered
      client.
```

This isn't the only message that you could see, but it will likely show a name, such as service1, followed by "junk" such as, M-PqM-Am-^?^C.

Since the memory returned is not necessarily zeroed, failing to null-terminate a string can cause unpredictable results. In this example, the string ended at the next zero(NULL) byte, well beyond the intended end of the string.

SOLUTION:

An application failing to null-terminate a string must be corrected.

The following statement was true in prior implementations, as well as the latest implementation of malloc():

> If a programmer wants to ensure that they receive a zero filled memory region, calloc() would be the correct function to use.

Here is an example of a coding error that could be seen:

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

#define LEN     8

main()
{
 char *name = "Tru64 UNIX";
 char *new_name;

 new_name = malloc(LEN);
 if(new_name == NULL) {
         perror("malloc()");
         exit(1);
 }
 strncpy(new_name, name, LEN);
 printf("The name is %s\n", new_name);
 }
```

Note in the above example that strncpy() will not be able to copy the whole string into the eight byte buffer. In this situation strncpy() does NOT put a NULL byte at the end of the string. This is a common usage error. The correct user code will give a length of one less than the buffer size to strncpy(), and manually store a zero in the last byte of the buffer, e.g.:

```
    #define LEN     9

      strncpy(new_name, name, LEN-1);
      new_name[LEN-1] = '\0';
```

ADDITIONAL COMMENTS:

Currently we have only seen this problem in two applications and we believe it will only be a few applications that have this type of coding error. Development engineering is reviewing the malloc() man pages to ensure they reflect the correct behavior of malloc().

KNOWN WORKAROUNDS:

1. For V4.0D/E, back out the complete BL12 patch kit, of course this will not work for V4.0F and V5.0 SSB.

   NOTE: DO NOT install patch kit BL12 then replace libc with the old libc.

2. Change the offending string to be one byte less than the allocated memory and terminate the string with a NULL.

```
*****************************< NOTE >************************************
*                                                                       *
* INFORMATION IN THIS DOCUMENT REPRESENTS OPERATIONAL EXPERIENCES AND   *
* SUGGESTIONS BY COMPAQ OR PARTNER EMPLOYEES.  COMPAQ SHALL NOT BE      *
* RESPONSIBLE FOR ANY ERRORS OR OMMISSIONS CONTAINED IN THIS DOCUMENT,  *
* AND RESERVES THE RIGHT TO MAKE CHANGES TO IT WITHOUT NOTICE.          *
*                                                                       *
*************************************************************************
```


```
<>UPDATE /TEXT_UPDATE/UNIQUE_IDENTIFIER="009DD99D-E4746860-1C02A1"-
 /TITLE="[TD 2696-CR] Application Problems after Patch Install and V4.0F/V5.0 - BLITZ
 /BADGE=(AUTHOR="999997",ENTER="913696",MODIFY="913696",-
 EDITORIAL_REVIEW="913696",TECHNICAL_REVIEW="999997")-
 /NAME=(AUTHOR="BONE HENRY",ENTER="SPAINHOWER JOE",-
 MODIFY="SPAINHOWER JOE",EDITORIAL_REVIEW="SPAINHOWER JOE",TECHNICAL_REVIEW="BONE HEN
 /DATE=(AUTHOR=" 3-SEP-1999",ENTER=" 3-SEP-1999",-
 EXPIRE=" 3-SEP-2001",FLASH=" 3-SEP-1999 14:33:46.69",MODIFY=" 3-SEP-1999",-
 EDITORIAL_REVIEW=" 3-SEP-1999",TECHNICAL_REVIEW=" 3-SEP-1999")-
 /GEOGRAPHY="USA"/SITE="EIRS"/OWNER="TIM-BLITZ"-
 /FLAGS=(USA_CUSTOMER_READABLE,NOPOST_MESSAGE_DISPLAY,NOLOCAL,-
 EUR_CUSTOMER_READABLE,GIA_CUSTOMER_READABLE,NOINIT_MESSAGE_DISPLAY,-
 EDITORIAL_REVIEWED,FIELD_READABLE,FLASH,TECHNICAL_REVIEWED,READY)
```