Speculation on how a mishandled 13-character string can result in a blue screen

devblogs.microsoft.com/oldnewthing/20090713-00

July 13, 2009

Raymond Chen

Commenter nolan reminisces about an old Windows 95 bug in the networking layer that crashed if a string was exactly 13 characters long. "So for the past 10 years or so, I've been wondering exactly how one could write code with that bug. Any bug that weird has to have a great story behind it."

I don't know what the story behind it is, but if after ten years you still can't imagine how such a bug could be possible, you don't have a very active imagination.

```
SomeFunction(char *hostname)
{
 char tmpbuffer[13]; // most host names are less than this size
 char *buffer;
 if (strlen(hostname) > sizeof(tmpbuffer)) {
   buffer = strdup(hostname);
   if (!buffer) return some error;
 } else {
   buffer = strcpy(tmpbuffer, hostname);
 }
 ... do stuff with buffer ...
 if (buffer != tmpbuffer) free(buffer);
}
```

If the host name is exactly 13 characters, then this code overflows the buffer by one character, corrupting the stack. A crash is hardly surprising at this point.

Raymond Chen

Follow