The TEMP directory is like a public hot tub whose water hasn’t been changed in over a year

devblogs.microsoft.com/oldnewthing/20121031-00

October 31, 2012

Raymond Chen

A customer reported that they couldn’t install product X. When they ran the installer, the got the error message

setup.exe – Application Error ×

The application was unable to start correctly (0xc00000ba). Click OK to close the application.

OK

The product X setup team weren’t sure what to make of this, and they asked if anybody had any ideas.

The error code `0xc00000ba` is `STATUS_FILE_IS_A_DIRECTORY`, which means that something was supposed to be a file, but instead it was a directory. The path-searching algorithm is not a backtracking algorithm, so once it finds something wrong, it just stops rather than backing up and trying the next directory.

This was enough of a clue to direct further investigation, which revealed that the customer had a *directory* named `C:\Users\Bob\AppData\Local\Temp\version.dll\`. The customer responded, “There are plenty of directories with names of DLLs in my TEMP directory, but getting rid of this one fixes the issue. Thanks!”

(Puzzle: Why are there so many directories with the names of DLLs? Psychic answer.)

I slipped something past you a little while back. Did you notice?

Okay, I gave it away in the subject line. The setup program is running from the TEMP directory. That should already set off alarm bells.

The TEMP directory is a dumping ground of random junk. A downloader may have put a DLL there and forgotten to delete it. (Or worse, expected it to stay there forever.) And that DLL might be from an incompatible version of some DLL your setup program uses. (I have seen applications ship their own custom versions of system DLLs! Yeah, because the x86 version of `shlwapi.dll` from Windows 2000 is drop-in compatible with the version of `shlwapi.dll` that comes with Windows 7.) Who knows what other yucky things have been lying around in that directory. Since the application directory is the first directory searched when the system looks for a DLL, a rogue DLL in the TEMP directory is a trap waiting to be sprung. (A similar issue applies to a shared Downloads directory.)

It's like the horror movie trope where the frightened pretty girl runs into a room, slams the door shut, then breathes a sigh of relief, believing herself to be safe. But she didn't check that the room was empty! (In other words, she created her airtight hatchway around an insecure room.)

The Program X setup team decided to change their installer so that it created a *subdirectory* of TEMP and extracted the main setup program there. That way, it got a fresh hot tub with clean water.

Remember, the directory is the application bundle. If you drop your application into a random directory, you've just added everything in that directory to your bundle. And if you don't secure your application directory, you're allowing anybody to add components to your bundle. That's one of the reasons why the Logo program encourages (requires?) applications to install into the Program Files directory: The ACLs on the Program Files directory allow write access only to administrators and installers. This makes the application bundle secure by default. If you want to make your application bundle insecure, you have to go out of your way.

Raymond Chen

Follow