Why does Windows Compressed Folders (Zip folders) reject paths that begin with a slash?

devblogs.microsoft.com/oldnewthing/20121010-00

Raymond Chen

A customer asked, "Does NTFS support files with a null string as the name?" No, NTFS does not support files with no name. None of the commonly-used Windows file systems do. Files must have a name. But what a strange question that is. The customer was kind enough to explain why they cared. "We have a zip file that the Compressed Folders (Zip folders) feature that comes with Windows cannot deal with. When we try to extract the contents of the zip file, we get the error message 'Windows has blocked access to these files to help protect your computer.' We've attached a copy of the file." The Compressed Folders functionality in Explorer has many known limitations, such as lack of support for ZIP64 and AES encryption. Neither of those applied to the zip file in question, however. The customer explained what they did. "We created the zip file with a third party zip tool. In particular, after adding a directory tree to the zip file, we renamed the root of the tree to have a blank name. In the zip file we sent you, we added A/file.txt, and then we used the zip tool to rename 'A' to the empty string." And indeed if you looked at the zip file in a hex editor, the file name was "/file.txt". Now the pieces fell into place. The Compressed Folders code was blocking the file because it was attempting to perform a directory traversal; specifically, it was trying to drop a file in the root directory. The ZIP Application Note says that the "file name" field consists of "The name of the file, with optional relative path." Note that the path must be relative. The next sentence emphasizes this point: "The path stored should not contain a drive or device letter, or leading slash." Therefore, the zip file is invalid, and the Compressed Folders code is within its rights to reject it. (And one wonders why the zip tool allowed the user to create an invalid zip file.)

It's unclear what the customer was trying to do by renaming "A" to the empty string. So the recommendation back to the customer was "Don't do that."

Raymond Chen

Follow