Quality updates: Consequences for rogue-patched binaries

devblogs.microsoft.com/oldnewthing/20200214-00

February 14, 2020

Raymond Chen

We spent the past week learning about the different types of Windows update packages, ending with the Quality update that obsoletes all the others.

The Quality update relies on the presence of a reverse patch that gets the files currently on the client machine back to the original versions, so that the forward patch can be applied to bring the file forward to the latest version.

This is bad news if you hacked the file by using a hex editor to patch some bytes.

Because patching the file on disk means that the reverse patch back to the original version won't work, and that makes the entire update fall apart. If you're lucky, the Quality update will fail to install, and you're not going to be able to make any progress until you un-patch the file back to its original form. If you're unlucky, the Quality update will apply the reverse patch anyway, creating a mess. (I don't know what will actually happen, and I'm not going to try it to find out.)

That's why when companies who develop fancy "system enhancement" software ask about patching files, we always say, "No, don't do it."

Since we know that nothing we say will stop them from proceeding with their plan to ship their "system enhancement" software, we ask them at least to limit their patching to in-memory copies of the file, and leave the file on disk unchanged.

Raymond Chen

Follow