PART 29

With what we have seen so far, we can try to, at least, analyze real programs. I will give you an exercise that I will solve in part 30. I would like you to take it as something funny and send me what you find.

The idea is that I give you two consecutive versions of a program, so there may be in the newer patches that can be found by diffing or analyzing. I advise you to do a diff as we saw in the previous parts and try to see if there are overflows and send it to me. It is not necessary to write code only to find vulnerable functions in which you want.

The installers are attached in their older and newer versions, perhaps the best thing would be installing the old version in a virtual machine and do a snapshot, then the new one and another snapshot, so you can extract the files to diff from both.

The idea is to have fun and play for a while no matter if you do it right or wrong.

You can see the CVE as help.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4654

The vulnerability is when you open a .ty extension file in VLC up to v0.94.

Ricardo Narvaja

Translated by: @IvinsonCLS