

Security FUD Leftovers

By *Roy Schestowitz*

Created *13/06/2019 - 7:44am*

Submitted by Roy Schestowitz on Thursday 13th of June 2019 07:44:36 AM Filed under [Security](#) [1]

- **[This is grim, Vim and Neovim: Opening this crafty file in your editor may pwn your box. Patch now if not already](#)**[2] [Ed: What utterly nonsensical sensationalism from El Reg (The Register). They make it sounds like the end of the world when it's difficult to exploit (you need to download a file). Focus on Windows back doors instead. Journalism in 2019 may be taking every small bug and making it look like a doomsday scenario; this merely discredits publications that do this.]
- **[If you haven?t patched Vim or NeoVim text editors, you really, really should](#)**[3] [Ed: Inevitably, drama queen Dan Goodin just had to grossly exaggerate the severity of this at Ars Technica. It's hard to exploit and not a big issue compared to proprietary software back doors.]
- **[macOS Security Will Never Stop Us From Running Software of Our Choice](#)**[4] [Ed: There's no "macOS Security"; Apple is a chronic liar on the subject (and was caught many times before). NSA PRISM, back doors and so on. It's all part of the design and the company routinely lies ("marketing").]

[Security](#)

Source URL: <http://www.tuxmachines.org/node/124836>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/59>

[2] https://www.theregister.co.uk/2019/06/12/vim_remote_command_execution_flaw/

[3] <https://arstechnica.com/information-technology/2019/06/if-you-havent-patched-vim-or-neovim-text-editors-you-really-really-should/>

[4] <https://www.macobserver.com/analysis/mac-os-security-not-burdensome/>