Solutions (there may be more possible answers, these are just examples):

1. This may not be the best course of action because it's generally preferred to use the responsible disclosure process where the vulnerability is disclosed privately for a specified period before being made public, so the company has a chance to fix it first. That way it reduces the window during which users are vulnerable. However, the friend may think it is the best course of action because perhaps they have knowledge that the company will not act in good faith to fix the bug and instead just hide it without addressing it, so an alternative option for getting the issue resolved is to publicize it immediately.
2. Good documentation can help thoroughly document the assumptions and known issues with a function or library. That way programmers can have more information about the limitations of a function, such as that `strncpy` doesn't add a null terminator.
3. One argument in support of this is the government has a responsibility to protect its citizens, and therefore according to views of partiality and partial cosmopolitanism we can argue that stockpiling vulnerabilities to aid in things like espionage for the state is acceptable even in the face of potential harms done to other groups as a result. One argument against this is the government should not preference the state and instead strive to treat people equally according to universal care or impartial benevolence. Stockpiling vulnerabilities harms certain individuals or groups in an attempt to preference state activities.