Programming Leftovers

By Roy Schestowitz
Created 25/06/2022 - 1:43pm
Submitted by Roy Schestowitz on Saturday 25th of June 2022 01:43:45 PM Filed under Development [1]

• [RFC] Zstandard as a second compression method to LLVM [2]

The LLVM project currently has support for zlib as a compression algorithm. Usage of it varies from compression of ELF debug sections, to serialization of performance stats and AST data structures.

We would like to add Zstandard (A.K.A. Zstd) as an alternative to zlib, which tends to achieve higher compression rates while being faster across the board. Using those for internal tooling could lead to speed improvements in places where we compress AST?s etc, without sacrificing the compressed size of them.

• Porting KCM modules from QtWidgets to QtQuick/Kirigami for GSOC 2022 [3]

I?ve been selected for GSOC this year. My task is to redesign and port the KCMs currently in Qt Widgets to QtQuick/Kirigami

Thanks, Nate and David for agreeing to mentor me.

• Rant: One day either JavaScript or AutoComplete will start www [4]

• Takedown Notice Wipes Game Boy Advance Emulator From GitHub [5]
A popular browser-based Game Boy Advance emulator with nearly 100 working games was removed from GitHub this week. The takedown request was sent by the ESA, which acts on behalf of Nintendo and other game companies. The problem hasn't been sorted out completely, however, as nostalgic games can easily find alternatives, even on GitHub.

Russia's Conti working on exploits for Intel ME BMC AMT IPMI ? Intel ME the biggest security fuck up in computing history ? sue Intel [6]

?The biggest network security threat today is a remote code execution exploit for Intel?s Management Engine.?

?Every computer with an Intel chipset produced in the last decade would be vulnerable to this exploit, and RCE would give an attacker full control over every aspect of a system.

If you want a metaphor, we are dinosaurs and an Intel ME exploit is an asteroid hurtling towards the Yucatán peninsula.? (https://hackaday.com/tag/intel-me/)

Intel might have installed ? over the course of at least a decade (to this day?) a closed source backdoor in your computer?s firmware, that might never receive updates and is hard to remove. Once this backdoor is fully cracked, everyone (Russia, China and North Korea) can use it. Having remote control over a server down to the BIOS is a neat feature.

[...]

another dramatic way to put it:

?The biggest network security threat today is a remote code execution exploit for Intel?s Management Engine.?

?Every computer with an Intel chipset produced in the last decade would be vulnerable to this exploit, and RCE would give an attacker full control over every aspect of a system.

Source URL: http://www.tuxmachines.org/node/166472

Links: