today's leftovers

By *Roy Schestowitz*
Created *28/02/2021 - 7:29pm*
Submitted by Roy Schestowitz on Sunday 28th of February 2021 07:29:39 PM Filed under Misc [1]

- **Snapcraft Clinic Successes [2]**

  On Thursday I mentioned we were restarting the Snapcraft Clinic. Basically we stand up a regular video call with engineers from the snap and snapcraft team & us from Snap Advocacy. Developers of applications and publishers of snaps are invited to join to troubleshoot.

  There was nothing especially secret or private discussed, but as we don?t record or stream the calls, and I don?t have direct permission to mention the applications or people involved, so I?ll keep this a little vague. In future I think we should ask permission and record the outcomes of the calls.

  We had a few productive discussions. One developer brought an application which they?d requested classic confinement for, and wished to discuss the options for confinement. We had a rather lengthy open discussion about the appropriateness of the available options. The developer was offered some choices, including making changes to their application to accomodate confinement, and another was (as always) not to snap the application. They appreciated our openness in terms of accepting that there are limitations with all software, and not everything always makes sense to be packaged as a snap, at the moment.

  We also had a productive discusison with a representative of a group responsible for publishing multiple snaps. They had difficulties with a graphical snapped application once it had been updated to use core20. The application would launch and almost immediately segfault. As the application was already published in the Snap Store, in a non-stable channel, we were all able to install it to test on our own systems.

- **Kraft Version 0.96 [3]**

Ich freue mich, heute das Release Version 0.96 von Kraft herauszugeben. Die neue Version kann über die Homepage heruntergeladen werden.

- **A new data format has landed in the upcoming GTG 0.5** **[4]**

  Diego?s changes are major, invasive technological changes, and they would benefit from extensive testing by everybody with ?real data? before 0.5 happens (very soon). I?ve done some pretty extensive testing & bug reporting in the last few months; Diego fixed all the issues I?ve reported so far, so I?ve pretty much run out of serious bugs now, as only a few remain targetted to the 0.5 milestone? But I?m only human, and it is possible that issues might remain, even after my troll-testing.

  Grab GTG?s git version ASAP, with a copy of your real data (for extra caution, and also because we want you to test with real data); see the instructions in the README, including the ?Where is my user data and config stored?? section.

  Please torture-test it to make sure everything is working properly, and report issues you may find (if any). Look for anything that might seem broken ?compared to 0.4?, incorrect task parenting/associations, incorrect tagging, broken content, etc.

- **MAS ?Ocean strainer? technology to be open source** **[5]**

  Inspired by the success of its ?Ocean Strainer? floating trash trap, a pilot project launched in the Dehiwala Canal last year, MAS Holdings will make the ?Ocean Strainer? technology available to interested parties, to replicate and scale up the solution.

- **Notes on Addressing Supply Chain Vulnerabilities** **[6]**

  One of the unsung achievements of modern software development is the degree to which it has become componentized: not that long ago, when you wanted to write a piece of software you had to write pretty much the whole thing using whatever tools were provided by the language you were writing in, maybe with a few specialized libraries like OpenSSL. No longer. The combination of newer languages, Open Source development and easy-to-use package management systems like JavaScript?s npm or Rust?s Cargo/crates.io has revolutionized how people write software, making it standard practice to pull in third party libraries even for the simplest tasks; it?s not at all uncommon for programs to depend on hundreds or thousands of third party packages.

  [...]

Even packages which are well maintained and have good development practices routinely have vulnerabilities. For example, Firefox recently released a new version that fixed a vulnerability in the popular ANGLE graphics engine, which is maintained by Google. Both Mozilla and Google follow the practices that this blog post recommends, but it?s just the case that people make mistakes. To (possibly mis)quote Steve Bellovin, ?Software has bugs. Security-relevant software has security-relevant bugs?. So, while these practices are important to reduce the risk of vulnerabilities, we know they can?t eliminate them.

Of course this applies to inadvertant vulnerabilities, but what about malicious actors (though note that Brewer et al. observe that ?Taking a step back, although supply-chain attacks are a risk, the vast majority of vulnerabilities are mundane and unintentional?honest errors made by well-intentioned developers.?)? It?s possible that some of their proposed changes (in particular forbidding anonymous authors) might have an impact here, but it?s really hard to see how this is actionable. What?s the standard for not being anonymous? That you have an e-mail address? A Web page? A DUNS number?[3] None of these seem particularly difficult for a dedicated attacker to fake and of course the more strict you make the requirements the more it?s a burden for the (vast majority) of legitimate developers.

I do want to acknowledge at this point that Brewer et al. clearly state that multiple layers of protection needed and that it?s necessary to have robust mechanisms for handling vulnerability defenses. I agree with all that, I?m just less certain about this particular piece.

- **26 Firefox Quantum About:Config Tricks You Need to Learn - Make Tech Easier [7]**

  ?Here be dragons,? reads the ominous disclaimer when you type about:config into Firefox?s URL bar, warning you that tweaking things in this area is largely experimental and can cause instability to your browser.

  Sounds exciting, right? And even though it sounds a little scary, the fact is you will almost certainly be okay when you start playing around in this area and can actually use the features here to improve and speed up your browser. These are Make Tech Easier?s favorite Firefox about:config tricks, freshly updated for Firefox Quantum.

- **Attackers collaborate to exploit CVE-2021-21972 and CVE-2021-21973 - Blueliv [8]**

Misc

Source URL: http://www.tuxmachines.org/node/148246

Links:
[1] http://www.tuxmachines.org/taxonomy/term/78
[2] https://popey.com/blog/2021/02/snapcraft-clinic-successes/
[3] https://tagfrei.wordpress.com/2021/02/27/kraft-version-0-96/

[4] https://fortintam.com/blog/gtg-data-format-v2-merged/
[5] http://www.sundayobserver.lk/2021/02/28/business/mas-%E2%80%98ocean-strainer%E2%80%99-technology-be-open-source
[6] https://blog.mozilla.org/blog/2021/02/27/notes-on-addressing-supply-chain-vulnerabilities/
[7] https://www.maketecheasier.com/28-coolest-firefox-aboutconfig-tricks/
[8] https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/attackers-collaborate-to-exploit-cve-2021-21972-and-cve-2021-21973/