Security leftovers

By Roy Schestowitz
Created 13/06/2022 - 2:55pm
Submitted by Roy Schestowitz on Monday 13th of June 2022 02:55:34 PM Filed under Security [1]

- **Security updates for Monday [LWN.net] [2]**

  Security updates have been issued by Debian (chromium, containerd, kernel, ntfs-3g, and vlc), Fedora (buildah and logrotate), Red Hat (xz), and SUSE (google-gson, netty3, rubygem-sinatra, and u-boot).

- **Cryptanalysis of ENCSecurity’s Encryption Implementation - Schneier on Security [3]**

  ENCSecurity markets a file encryption system, and it’s used by SanDisk, Sony, Lexar, and probably others. Despite it using AES as its algorithm, it’s implementation is flawed in multiple ways?and breakable.

- **Practical bruteforce of AES-1024 military grade encryption ? Kudelski Security Research [4] [Ed: Proprietary software is not military-grade, it is degraded; Encryption that works isn’t difficult to implement, but it makes your life and your project difficult because states begin to interfere and demand back doors]**

  I recently presented work on the analysis of a file encryption solution that claimed to implement ?AES-1024 military grade encryption?. Spoiler alert: I did not break AES, and this work does not concern the security of AES. You may find advanced research regarding this topic.

  This project started during a forensic analysis. One of my colleagues came with a USB stick containing a vault encrypted with SanDisk Secure Access software. He asked me if it was
possible to brute force the password of the vault to recover the content. I did not know this software thus, I started to research. It appeared that this solution is distributed by Sandisk by default on any storage device you buy from them.

- **7 simple bot detection methods that won't inconvenience users** [5]

  Millions of (poorly coded) bots relentlessly crawl the web to detect and spew junk content into any form they find. The go-to countermeasure is to force everyone to complete a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA).

- **Kubernetes security risks that keep developers up at night** [6]

  In a recent Red Hat survey of more than 300 production-level Kubernetes users, 93% of respondents admitted to experiencing at least one security incident in their Kubernetes environments during the previous year?and 31% of respondents say they experienced revenue or customer loss during that year as a consequence.

  Our industry can do better. This article summarizes findings from the survey, reported in our 2022 State of Kubernetes security report, and highlights the weak points of Kubernetes security today along with a path forward involving DevSecOps.

---

**Security**

**Source URL:** [http://www.tuxmachines.org/node/165956](http://www.tuxmachines.org/node/165956)

**Links:**
[1] [http://www.tuxmachines.org/taxonomy/term/59](http://www.tuxmachines.org/taxonomy/term/59)
[2] [https://lwn.net/Articles/897711/](https://lwn.net/Articles/897711/)
[6] [https://developers.redhat.com/articles/2022/06/13/kubernetes-security-risks-keep-developers-night](https://developers.redhat.com/articles/2022/06/13/kubernetes-security-risks-keep-developers-night)