Security Leftovers

By Roy Schestowitz
Created 23/08/2021 - 5:17pm
Submitted by Roy Schestowitz on Monday 23rd of August 2021 05:17:33 PM Filed under Security [1]

- Security updates for Monday [LWN.net] [2]
  Security updates have been issued by Debian (ffmpeg, ircii, and scrollz), Fedora (kernel, krb5, libX11, and rust-actix-http), Mageia (kernel and kernel-linus), openSUSE (aspell, chromium, dbus-1, isync, java-1_8_0-openjdk, krb5, libass, libhts, libvirt, prosody, systemd, and tor), SUSE (cpio, dbus-1, libvirt, php7, qemu, and systemd), and Ubuntu (inetutils).

- Top 15 Vulnerabilities Attackers Exploited Millions of Times to Hack Linux Systems [3] [Ed: This headline is false; it conflates attempts with successful cracking, and it wrongly attributes everything to "Linux"; this isn't "Hacker News" but Microsoft spin/deflection]
  Close to 14 million Linux-based systems are directly exposed to the Internet, making them a lucrative target for an array of real-world attacks that could result in the deployment of malicious web shells, coin miners, ransomware, and other trojans.

  That's according to an in-depth look at the Linux threat landscape published by U.S.-Japanese cybersecurity firm Trend Micro, detailing the top threats and vulnerabilities affecting the operating system in the first half of 2021, based on data amassed from honeypots, sensors, and anonymized telemetry.

- Kubernetes hardening: Drilling down on the NSA/CISA guidance [4] [Ed: Far too much back doors proponents' influence inside Kubernetes (Microsoft, Google, IBM...), so this bundle of complexity is unlikely to yield real rather than perceived security gains]
Kubernetes has become the de facto choice for container orchestration. Some studies report that up to 88% of organizations are using Kubernetes for their container orchestration needs and 74% of that occurring in production environments. That said, security remains a critical concern with as many as 94% of organizations reporting at least one security incident in their Kubernetes environments in the last 12 months.

As organizations continue to adopt Kubernetes, it is crucial that they follow industry best practices and guidance to ensure they are using Kubernetes securely. One great resource is the Kubernetes Hardening Guidance recently published by the US National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA).

Real-time Analytics News for Week Ending August 21 - RTInsights [5]

Ubuntu received the FIPS 140-2, Level 1 certification for its cryptographic modules in Ubuntu 20.04 LTS, including OpenSSL 1.1.1. This certification is built on Canonical’s track record in designing Ubuntu for high security and regulated workloads that powers U.S government agencies, prime contractors, service providers, and organizations in regulated industries, including healthcare and finance.