Security and Proprietary Software

By Roy Schestowitz
Created 08/11/2021 - 5:31pm

Security updates for Monday [3]

Security updates have been issued by Debian (containerd, redis, and sqlalchemy), Fedora (kernel, radeontop, rpki-client, and webkit2gtk3), openSUSE (java-1_8_0-openj9, libvirt, mailman, transfig, and webkit2gtk3), Oracle (thunderbird), SUSE (libvirt), and Ubuntu (icu).

Tips to Enhance Linux Security [4]

In recent years, the usage of linux operating systems has increased a bit. Though, not at that impressive rate, there have been more users shifting towards Linux based systems. And around 50% of the internet users are running some sort of Linux flavor on their systems.

There was a time when Linux users would consider themselves as the lucky souls who were not afraid of cyber-attacks or other kinds of vulnerabilities.

But it is no secret that the Linux server has become one of today's most desirable targets. The past few years have seen emerging malware strains that demonstrate new and dangerous tactics for spreading, remaining undetected on your machine?Cloud Snooper, EvilGnome just to name a couple!

This post is going to elaborate you with some knowledge on how Linux servers are being targeted by malware, rootkits and other malicious attacks. And above all what are the sure shot ways to improve security of Linux systems.
Microsoft's expired cert brings these Windows apps to their knees. - Invidious [5]

Microsoft will now snitch on you at work like never before [6]

I feel sure there are many American workers who have put the whistle in their mouths, like former Facebook employee Frances Haugen, but been too afraid to blow it.

[…]

The first is headlined: "Microsoft 365 compliance center: Insider risk management -- Increased visibility on browsers."

It all sounded wonderful until you those last four words, didn't it? For this is the roadmap for administrators. And when you give a kindly administrator "increased visibility on browsers," you can feel sure this means an elevated level of surveillance of what employees are typing into those browsers.

In this case, Microsoft is targeting "risky activity." Which, presumably, has some sort of definition. It offers a link to its compliance center, where the very first sentence has whistleblower built in: "Web browsers are often used by users to access both sensitive and non-sensitive files within an organization."

And what is the compliance center monitoring? Why, "files copied to personal cloud storage, files printed to local or network devices, files transferred or copied to a network share, files copied to USB devices."

You always assumed this was the case? Perhaps. But now there will be mysteriously increased visibility.

"How might this visibility be increased?," I hear you shudder. Well, there's another little roadmap update that may, just may, offer a clue.

Source URL: http://www.tuxmachines.org/node/157690

Links:
[3] https://lwn.net/Articles/875420/rss