

Security: Patches, Whonix, IPFire and More

By *Roy Schestowitz*

Created 27/02/2020 - 6:54pm

Submitted by Roy Schestowitz on Thursday 27th of February 2020 06:54:30 PM Filed under [Security](#) [1]

- [Security updates for Thursday](#) [2]

Security updates have been issued by CentOS (kernel, ksh, python-pillow, and thunderbird), Debian (opensmtpd, proftpd-dfsg, and rake), Fedora (NetworkManager-ssh), openSUSE (chromium), and SUSE (libexif, mariadb, ovmf, python3, and squid).

- [Whonix VirtualBox 15.0.0.8.9 - Point Release! - vanguards; TCP ISN Leak Protection; Extensive Hardening!](#) [3]

This is a point release.

Download Whonix for VirtualBox:

- [Build your career in Computer Forensics: List of Digital Forensic Tools - Part I](#)[4]

Digital devices are present everywhere and considered to be the primary source of evidence in the case of cybercrime. Out of all the devices, phones and laptops are the top weapons used in cybercrimes. Regardless of who the device belonged to, either the victim or suspect, it offers an abundance of data to investigate the crime. But retrieving evidence from these devices in a secure environment can be very challenging. To overcome the time constraint and other complications, cyber forensic professionals use digital forensic tools.

- [What are Open Source Security Approaches? With Examples](#) [5]

Open source security approaches enable organizations to secure their applications and networks while avoiding expensive proprietary security offerings.

An open source approach allows organizations to secure their applications across cloud providers and other platforms using platform-agnostic APIs. These APIs are written by contributors to the open source software code while cloud providers may use open source code that allows the open APIs to connect to the cloud.

Open source approaches, for security or not, also bring in collaboration across an industry. It isn't just one organization that benefits from a program or technology, but everyone who contributes to and uses it.

The open source projects and programs used as examples in this article come from two major open source entities: The Linux Foundation and the Cloud Native Computing Foundation (CNCF). The two also work closely together to further the projects under their purview.

- [Cloud Snooper: Hackers Using Linux Kernel Driver To Attack Cloud Server](#) [6] [Ed: So, if you install malicious software in Linux, due to recklessness or sabotage, it'll do malicious things. How is that a Linux weakness?]

Whether you're a Linux user or not, you must have heard the buzzword about the Linux ? Best OS for security.? Well, it is true, but being a computer program, Linux also has some downside that challenges its security.

Talking about the security risks, recently, SophosLab published a report about a new malware dubbed Cloud Snooper, that can compromise the security of any Linux or other OS based servers by deploying a kernel driver.

- [IPFire on AWS: Update to IPFire 2.25 - Core Update 141](#) [7]

Today, we have updated IPFire on AWS to IPFire 2.25 - Core Update 141 - the latest official release of IPFire.

Since IPFire is available on AWS, we are gaining more and more users who are securing their cloud infrastructure behind an easy to configure, yet fast and secure firewall.

This update adds the rewritten DNS stack and brings many bug fixes to the cloud.

[Security](#)

Source URL: <http://www.tuxmachines.org/node/134565>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/59>

[2] <https://lwn.net/Articles/813431/rss>

[3] <https://forums.whonix.org/t/whonix-virtualbox-15-0-0-8-9-point-release-vanguards-tcp-isn-leak-protection-extensive-hardening/8994>

[4] <https://blog.eccouncil.org/build-your-career-in-computer-forensics-list-of-digital-forensic-tools-part-i/>

[5] <https://www.sdxcentral.com/open-source/definitions/what-are-open-source-security-approaches-with-examples/>

[6] <https://fossbytes.com/cloud-snooper-hackers-linux-kernel-driver-attack-cloud-server/>

[7] <https://blog.ipfire.org/post/ipfire-on-aws-update-to-ipfire-2-25-core-update-141>