Security: Linux, Docker and Guix

By *Roy Schestowitz*
Created *18/10/2019 - 5:38am*
Submitted by Roy Schestowitz on Friday 18th of October 2019 05:38:53 AM Filed under Security [1]

- **Unpatched Linux bug may open devices to serious attacks over Wi-Fi [2]**

  > The flaw is located in the RTLWIFI driver, which is used to support Realtek Wi-Fi chips in Linux devices. The vulnerability triggers a buffer overflow in the Linux kernel when a machine with a Realtek Wi-Fi chip is within radio range of a malicious device. At a minimum, exploits would cause an operating-system crash and could possibly allow a hacker to gain complete control of the computer. The flaw dates back to version 3.10.1 of the Linux kernel released in 2013.

- **Docker Attack Worm Mines for Monero [3]**

- **Insecure permissions on profile directory (CVE-2019-18192) [4]**

  > We have become aware of a security issue for Guix on multi-user systems that we have just fixed (CVE-2019-18192). Anyone running Guix on a multi-user system is encouraged to upgrade guix-daemon?see below for instructions.
  >
  > **Context**
  >
  > The default user profile, ~/.guix-profile, points to /var/guix/profiles/per-user/$USER. Until now, /var/guix/profiles/per-user was world-writable, allowing the guix command to create the $USER sub-directory.
  >
  > On a multi-user system, this allowed a malicious user to create and populate that $USER sub-directory for another user that had not yet logged in. Since /var/?/$USER is in $PATH, the

target user could end up running attacker-provided code. See the bug report for more information.

This issue was initially reported by Michael Orlitzky for Nix (CVE-2019-17365).

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://arstechnica.com/information-technology/2019/10/unpatched-linux-flaw-may-let-attackers-crash-or-compromise-nearby-devices/
[3] https://www.sdxcentral.com/articles/news/docker-attack-worm-mines-for-monero/2019/10/
[4] https://guix.gnu.org/blog/2019/insecure-permissions-on-profile-directory-cve-2019-18192/