# Security Leftovers

By *Roy Schestowitz*
Created *26/07/2021 - 7:00pm*
Submitted by Roy Schestowitz on Monday 26th of July 2021 07:00:25 PM Filed under Security [1]

- **Security updates for Monday [2]**

  Security updates have been issued by Debian (aspell, intel-microcode, krb5, rabbitmq-server, and ruby-actionpack-page-caching), Fedora (chromium, containernetworking-plugins, containers-common, crun, fossil, podman, skopeo, varnish-modules, and vmod-uuid), Gentoo (leptonica, libsdl2, and libyang), Mageia (golang, lib3mf, nodejs, python-pip, redis, and xstream), openSUSE (containerd, crmsh, curl, icinga2, and systemd), Oracle (containerd), and Red Hat (thunderbird).

- **Running FIPS 140 workloads on Ubuntu | Ubuntu [3]**

  Even though cryptography is used by almost every application today, the implementation of it is usually delegated to specialized cryptographic libraries. There are multiple reasons for that, including that implementing cryptography is not easy, and in fact it is easy to get wrong. Small mistakes?such as reusing a nonce?may render the data encrypted by an application recognizable. At the same time, the security landscape changes so fast that secure software of 10 years ago can no longer withstand attacks that exploit newly discovered vulnerabilities. For instance, algorithms like RC4 that were dominant in the early days of Internet commerce are today considered broken.

  How can we be assured that these cryptographic applications and libraries implement cryptography correctly and follow best practices such as not using legacy cryptography? As cryptography is sensitive to governments around the world, there is no universally accepted answer yet. To address this problem in the U.S., NIST developed FIPS 140, a data protection standard that is our focus in this article.

  FIPS 140 defines security requirements related to the design and implementation of a

cryptographic module, or in software terms, for an application or library implementing cryptography. The standard has multiple levels of security, from levels 1 to 4, with level 1 applying to software implementations, while level 2 and further applying to specialized hardware alongside its software. On level 1, the standard requires the use of known, secure cryptographic algorithms and modes for data protection and requires their logical separation from the application. It further includes a certification process that ensures that the claims are tested and attested by an accredited lab by NIST.

In essence the FIPS 140 standard ensures that cryptography is implemented using well known secure designs, follows certain best practices, does not involve obscure algorithms, and that there is a due process in attestation.

- **Renewed FIPS 140-2 Validation For Red Hat Enterprise Linux 8.2 | TFiR: Interviews, News & Analysis by Swapnil Bhartiya** **[4]**

  Red Hat has announced the renewal of the Federal Information Processing Standard 140-2 (FIPS 140-2) security validation for Red Hat Enterprise Linux 8.2. The second FIPS certification for the Red Hat Enterprise Linux 8 platform, this validation indicates Red Hat?s leadership and commitment to providing a more secure backbone for the innovation of open hybrid cloud.

  With this validation for Red Hat Enterprise Linux 8.2, many of Red Hat?s open hybrid cloud offerings also retain the FIPS 140-2 certification as layered products building on Red Hat Enterprise Linux 8.2?s cryptography modules. These include but are not limited to: Red Hat Ceph Storage, Red Hat Gluster Storage, Red Hat OpenShift, Red Hat OpenStack Platform, Red Hat Satellite, and Red Hat Virtualization.

- **The 10 Best Tools to Scan Your Linux Server for Malware and Security Flaws** **[5]**

  Linux is downright one of the most popular and secure operating systems for large-scale servers. Despite its widespread usage, it remains vulnerable to cyberattacks. Hackers target servers to either shut them down or steal valuable information.

  There is a pressing need to develop counter-hacking methods to brace security breaches and malware attacks. This is possible by hiring cybersecurity professionals; unfortunately, this can prove to be a costly affair. The next best solution is to install scanning tools that fit like a hand in glove for your Linux systems.

Security

---



**Links:**

[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/864346/rss
[3] https://ubuntu.com//blog/running-fips-140-workloads-on-ubuntu
[4] https://www.tfir.io/renewed-fips-140-2-validation-for-red-hat-enterprise-linux-8-2/
[5] https://www.makeuseof.com/best-tools-to-scan-linux-server-malware-and-security-flaws/