Published on *Tux Machines* (http://www.tuxmachines.org)

Security: Software Updates, Kali NetHunter Updates, OpenWRT Bug and Scams That Exploit COVID-19

By *Roy Schestowitz*
Created *01/04/2020 - 11:01pm*
Submitted by Roy Schestowitz on Wednesday 1st of April 2020 11:01:29 PM Filed under Security [1]

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

  > Security updates have been issued by Debian (apng2gif, gst-plugins-bad0.10, and libpam-krb5), Fedora (coturn, libarchive, and phpMyAdmin), Mageia (chromium-browser-stable, nghttp2, php, phpmyadmin, sympa, and vim), openSUSE (GraphicsMagick, ldns, phpMyAdmin, python-mysql-connector-python, python-nltk, and tor), Red Hat (advancecomp, avahi, bash, bind, bluez, buildah, chromium-browser, cups, curl, docker, dovecot, doxygen, dpdk, evolution, expat, file, gettext, GNOME, httpd, idm:DL1, ImageMagick, kernel, kernel-rt, lftp, libosinfo, libqb, libreoffice, libsndfile, libxml2, mailman, mariadb, mod_auth_mellon, mutt, nbdkit, net-snmp, nss-softokn, okular, php, podman, polkit, poppler and evince, procps-ng, python, python-twisted-web, python3, qemu-kvm, qemu-kvm-ma, qt, rsyslog, samba, skopeo, squid, systemd, taglib, texlive, unzip, virt:8.1, wireshark, and zziplib), Slackware (gnutls and httpd), and SUSE (glibc, icu, kernel, and mariadb).

- **Kali NetHunter Updates [3]**

  > Many outstanding discoveries have been made by our vibrant NetHunter community since 2020.1, so we have decided to publish a mid-term release to showcase these amazing developments on selected devices.
  >
  > [..].
  >
  > The Android 8.1 image is considered the recommended release with a proven track record of supporting NetHunter under the most extreme conditions, including force encryption of the

data partition.

Considering the current maturity of Android 10 for this platform, we would consider this version to be most suited for those who love to experiment and don?t mind getting things working by themselves. We had to edit the vendor fstab file on a laptop to disable force encryption because TWRP didn?t support it at the time of writing. If that doesn?t scare you then this image might be just right for you.

- **OpenWRT code-execution bug puts millions of devices at risk [4]**

For almost three years, OpenWRT?the open source operating system that powers home routers and other types of embedded systems?has been vulnerable to remote code-execution attacks because updates were delivered over an unencrypted channel and digital signature verifications are easy to bypass, a researcher said.

OpenWRT has a loyal base of users who use the freely available package as an alternative to the firmware that comes installed on their devices. Besides routers, OpenWRT runs on smartphones, pocket computers and even laptops and desktop PCs. Users generally find OpenWRT to be a more secure choice because it offers advanced functions and its source code is easy to audit.

[...]

These code-execution exploits are limited in their scope because adversaries must either be in a position to conduct a man-in-the-middle attack or tamper with the DNS server that a device uses to find the update on the Internet. That means routers on a network that has no malicious users and using a legitimate DNS server are safe from attack. Vranken also speculates that packet spoofing or ARP cache poisoning may also make attacks possible, but he cautions that he didn?t test either method.

Despite the requirements, many networks connect people who are unknown or untrusted by the device operator. What?s more, attacks that replace router settings pointing to a legitimate DNS to a malicious one are a fact of life on the Internet, as in-the-wild attack here, here, here, and here (to name just a few) demonstrate.

- **OpenWRT code-execution bug puts millions of devices at risk [5]**

The headline may be a bit overwrought, though.

- **How Hackers Are Targeting Networks Amidst Coronavirus Threat? [6]**

There is no doubt that COVID-19 has created fear, panic and uncertainty among the public, but it has also opened new possibilities for hackers to increase cyber attacks using different approaches. According to reports in the last few weeks, hackers are taking advantage of the current situation to spread fake news about important information related to government notices, school closures, health risks etc.

Security

Source URL: http://www.tuxmachines.org/node/135883

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/816511/rss
[3] https://www.kali.org/news/kali-nethunter-updates/
[4] https://arstechnica.com/information-technology/2020/03/openwrt-is-vulnerable-to-attacks-that-execute-malicious-code/
[5] https://lwn.net/Articles/816516/rss
[6] https://linuxtechlab.com/how-hackers-are-targeting-networks-amidst-coronavirus-threat/