Security Leftovers

By *Roy Schestowitz*
Created *06/04/2020 - 4:03pm*
Submitted by Roy Schestowitz on Monday 6th of April 2020 04:03:10 PM Filed under Security [1]

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

  Security updates have been issued by Debian (firefox-esr, gnutls28, and libmtp), Fedora (cyrus-sasl, firefox, glibc, squid, and telnet), Gentoo (firefox), Mageia (dcraw, firefox, kernel, kernel-linus, librsvg, and python-nltk), openSUSE (firefox, haproxy, icu, and spamassassin), Red Hat (nodejs:10, openstack-manila, python-django, python-XStatic-jQuery, and telnet), Slackware (firefox), SUSE (bluez, exiv2, and libxslt), and Ubuntu (firefox).

- **Open Source Security Podcast: Episode 191 - Security scanners are all terrible** **[3]**

  Josh and Kurt talk about security scanners. They're all pretty bad today, but there are some things we can do to make them better. Step one is to understand the problem. Do you know why you're running the scanner and what the reports mean?

- **Misconfigured Docker API Ports Targeted by Kinsing Malware** **[4]**

  Security researchers observed an attack campaign that targeted misconfigured Docker API ports with samples of Kinsing malware.

  According to Aqua Security, the campaign began when it capitalized on an unprotected Docker API port to run a Ubuntu container.

  The command used for creating the Ubuntu container included a shell script ?d.sh.? By means

of its 600+ lines of code, the shell script began by disabling security measures, clearing logs and disabling other malware and cryptominer samples. It?s then that the command killed rival malicious Docker containers before loading its Kinsing payload.

- **L1d Cache Flush On Context Switch Moves Forward For Linux In Light Of Vulnerabilities [5]**

  A new patch series sent out just under one month ago was providing opt-in L1 data cache flushing on context switching. That work has now been revived again and now with documentation added it's clear that this work is being done in response to a recent CVE being made public.

  The patches originally sent out by an Amazon engineer characterized the work as for the "paranoid due to the recent snoop assisted data sampling vulnerabilities, to flush their L1D on being switched out. This protects their data from being snooped or leaked via side channels after the task has context switched out."

Security

Source URL: http://www.tuxmachines.org/node/136078

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/816886/rss
[3] http://www.opensourcesecuritypodcast.com/2020/04/episode-191-security-scanners-are-all.html
[4] https://www.tripwire.com/state-of-security/security-data-protection/cloud/misconfigured-docker-api-ports-targeted-by-kinsing-malware/
[5] https://www.phoronix.com/scan.php?page=news_item&px=L1d-Flush-Ctx-Switch-April