Security: Updates, Containers, Compilers and More

By *Roy Schestowitz*
Created *19/06/2019 - 4:56pm*
Submitted by Roy Schestowitz on Wednesday 19th of June 2019 04:56:44 PM Filed under Security [1]

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

- **Containers pose security risks, but mitigation isn't tough: Lees** **[3]**

  Recent concerns over the security offered by containers are not unjustified, the chief technologist for Germany-based SUSE in the Asia-Pacific says, adding however that there are a lot of operational things that could be done to mitigate the risk.

  Peter Lees told iTWire in response to queries that the whole point of containers was to be able to get new functionality out quickly. "And in modern development that often means gluing together micro-services from many different sources, which in turn could mean that the ultimate source of those functions may not have been vetted," he said.

  Container security was in the limelight in April when the credentials of some 190,000 account holders at Docker Hub, the official repository for Docker container images, were exposed due to "a brief moment of unauthorised access".

- **Ubuntu 19.10 To Harden Its Compiler With Stack Clash Protection & Intel CET** **[4]**

  In addition to discontinuing i386 support, Canonical announced another change being worked on for Ubuntu 19.10 is compiler hardening.

  In the name of increased security, their GCC 9 compiler for Ubuntu 19.10 will have some additional tunables enabled: -fstack-clash-protection and -fcf-protection.

> The stack clash protection is designed to fend off stack clash attacks by checking pages at allocation-time that instead would result in ideally just a segmentation fault.

- **What Red Hat OpenShift Online and OpenShift Dedicated customers should know about June 2019 kernel network stack flaws** **[5]**

- **Netflix Finds Bug That Creates Linux Kernel Panic** **[6]**

- **Docker Is Porting Its Container Platform to Microsoft Windows Subsystem for Linux 2, Ubuntu 19.10 Will Drop 32-Bit Builds, Children of Morta Still Coming to Linux and Vulnerabilities Discovered in the Linux TCP System** **[7]**

> Security researchers over at Netflix uncovered some troubling security vulnerabilities inside the Linux (and FreeBSD) TCP subsystem, the worst of which is being called SACK. It can permit remote attackers to induce a kernel panic from within your Linux operating system. Patches are available for affected Linux distributions.

Security

Source URL: http://www.tuxmachines.org/node/125051

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/791462/rss
[3] https://www.itwire.com/open-source/containers-pose-security-risks,-but-mitigation-isn-t-tough-lees.html
[4] https://www.phoronix.com/scan.php?page=news_item&px=Ubuntu-19.10-GCC-Hardening
[5] https://blog.openshift.com/what-red-hat-openshift-online-and-openshift-dedicated-customers-should-know-about-june-2019-kernel-network-stack-flaws/
[6] https://www.itprotoday.com/linux/netflix-finds-bug-creates-linux-kernel-panic
[7] https://www.linuxjournal.com/content/docker-porting-its-container-platform-microsoft-windows-subsystem-linux-2-ubuntu-1910-will