Security Leftovers

By Roy Schestowitz
Created 01/04/2020 - 4:21am
Submitted by Roy Schestowitz on Wednesday 1st of April 2020 04:21:16 AM Filed under Security [1]

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

  Security updates have been issued by Debian (tinyproxy), Fedora (okular), Gentoo (ffmpeg, libxls, and qemu), openSUSE (GraphicsMagick), Red Hat (qemu-kvm-rhev), SUSE (cloud-init and spamassassin), and Ubuntu (bluez, libpam-krb5, linux-raspi2, linux-raspi2-5.3, and Timeshift).

- **Why Understanding CVEs Is Critical for Data Scientists** [3]

  CVEs are Common Vulnerabilities and Exposures found in software components. Because modern software is complex with its many layers, interdependencies, data input, and libraries, vulnerabilities tend to emerge over time. Ignoring a high CVE score can result in security breaches and unstable applications.

  Because data scientists work with vast stores of data, they need to take responsibility for the software components they use to minimize risk and protect customer data. A golden rule in security is, wherever valuable data can be found, hackers will go.

  Software developers refer to CVE databases and scores on a regular basis to minimize the risk of using vulnerable components (packages and binaries) in their applications or web pages. They also monitor for vulnerabilities in components they currently use. To reduce the risk of a security breach from open-source packages, data science teams need to take this page from the software developer’s playbook and apply it to their data science and machine learning pipeline.
pam-krb5 4.9 [4]

This is a security release fixing a one-byte buffer overflow when relaying prompts from the underlying Kerberos library. All users of my pam-krb5 module should upgrade as soon as possible. See the security advisory for more information.

There are also a couple more minor security improvements in this release: The module now rejects passwords as long or longer than PAM_MAX_RESP_SIZE (normally 512 octets) since they can be a denial of service attack via the Kerberos string-to-key function, and uses explicit_bzero where available to clear passwords before releasing memory.

* rethinking openbsd security [5]

OpenBSD aims to be a secure operating system. In the past few months there were quite a few security errata, however. That's not too unusual, but some of the recent ones were a bit special. One might even say bad. The OpenBSD approach to security has a few aspects, two of which might be avoiding errors and minimizing the risk of mistakes. Other people have other ideas about how to build secure systems. I think it's worth examining whether the OpenBSD approach works, or if this is evidence that it's doomed to failure.

Source URL: [http://www.tuxmachines.org/node/135846](http://www.tuxmachines.org/node/135846)

Links:
[2] https://lwn.net/Articles/816368/rss