Security Leftovers

By *Roy Schestowitz*
Created *17/07/2019 - 3:43am*
Submitted by Roy Schestowitz on Wednesday 17th of July 2019 03:43:52 AM Filed under Security [1]

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

  Security updates have been issued by Fedora (expat and radare2), Oracle (thunderbird), Red Hat (389-ds-base, keepalived, libssh2, perl, and vim), Scientific Linux (thunderbird), SUSE (bzip2, kernel, podofo, systemd, webkit2gtk3, and xrdp), and Ubuntu (bash, nss, redis, squid, squid3, and Zipios).

- **Explainer: What is post-quantum cryptography? [3]**

  Few of us give much thought to the tiny padlock symbol that appears in our web browsers every time we use an e-commerce site, send and receive emails, or check our bank or credit card accounts. But it?s a signal that the online services are using HTTPS, a web protocol that encrypts the data we send across the internet and the responses we receive. This and other forms of encryption protect all kinds of electronic communications, as well as things like passwords, digital signatures, and health records.

- **Monitoring Linux Logs with Kibana and Rsyslog [4]**

  f you are a system administrator, or even a curious application developer, there is a high chance that you are regularly digging into your logs to find precious information in them.

  Sometimes you may want to monitor SSH intrusions on your VMs.

  Sometimes, you might want to see what errors were raised by your application server on a

certain day, on a very specific hour. Or you may want to have some insights about who stopped your systemd service on one of your VMs.

If you pictured yourself in one of those points, you are probably on the right tutorial.

In this tutorial, we are to build a complete log monitoring pipeline using the ELK stack (ElasticSearch, Logstash and Kibana) and Rsyslog as a powerful syslog server.

Before going any further, and jumping into technical considerations right away, let?s have a talk about why do we want to monitor Linux logs with Kibana.

- **Critical Vulnerability Found In Ad Inserter WordPress Plugin [5] [Ed: Well, ads are malicious, many are literally malware, so people who put this crap in their site ask for if not deserve the worst.]**

  On July 12, Wordfence team(Another popular security plugin for WordPress), discovered a vulnerability called RCE ? Remote Code Execution in Ad inserter. This vulnerability can allow an attacker to run any arbitrary PHP code on the site.

  The vulnerability was found in Ad preview module of the plugin where you can preview the ads position, size, etc. before publishing it. This action can only be executed by the WordPress administrators and to ensure this, the plugin writer used WordPress function ?check_admin_referer()? which ensures that the action is being performed by the administrator.

  Wordfence threat intelligence team who discovered this vulnerability said the ?check_admin_referer()? function is not enough protection. check_admin_referer() is designed to protect against CSRF (Cross-site request forgery) and the way it ensures this is by checking if nonce (a one-time token) exists in the request.

- **Wanna work on Debian LTS (and get funded)? [6]**

  If you are in Curitiba and are interested to work on Debian LTS (and get paid for that work), please come and talk to me, Debian LTS is still looking for more contributors!

Security

Source URL: http://www.tuxmachines.org/node/125973

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/793852/rss
[3] https://linuxsecurity.com/news/cryptography/explainer-what-is-post-quantum-cryptography
[4] http://devconnected.com/monitoring-linux-logs-with-kibana-and-rsyslog/
[5] http://www.linuxandubuntu.com/home/critical-vulnerability-found-in-ad-inserter

[6] http://layer-acht.org/thinking/blog/20190716-wanna-work-on-lts/