Security Leftovers

By *Roy Schestowitz*
Created *14/06/2019 - 8:02am*
Submitted by Roy Schestowitz on Friday 14th of June 2019 08:02:13 AM Filed under Security [1]

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

- **WSL2 and Kali** **[3]**

- **Security service tracks embedded Linux vulnerabilities** **[4]**

  > Timesys has launched a Vigiles security monitoring and management platform with CVE tracking for embedded Linux available as free software or as a subscription service.
  >
  > Timesys Vigiles automates the identification, tracking, and analysis of vulnerabilities by comparing embedded Linux firmware with NIST?s daily Common Vulnerabilities and Exposures (CVE) notifications. The software helps customers focus on vulnerabilities that pose the biggest threats to a customer?s specific software components, thereby ?eliminating the need to manually monitor and analyze thousands of vulnerabilities,? says Timesys.

- **Vim devs fix system-pwning text editor bug** **[5] [Ed: This requires obtaining and opening malicious files though]**

  > The attack exploits a vulnerability in a Vim feature called modelines, which lets you set variables specific to a file. As long as these statements are in the first few lines, Vim interprets them as instructions. They might tell Vim to display the file with a text width of 60 characters, for example. Or maybe you want to expand tabs to spaces to avoid another geek?s ire.

- **Mail servers running Exim come under attack [6]**

  Mail servers running the Exim mail transport agent are being exploited, with the attackers using a vulnerability disclosed a few days ago to run arbitrary commands as root, a security practitioner has warned.

  Exim, one of the four MTAs commonly used on Unix servers, is developed by Phillip Hazel at the University of Cambridge. It is the default on some Linux distributions, like Debian.

  [...]

  The original post about the vulnerability was released by Qualys Research Labs on 5 June, which said it was trivially exploitable in local and non-default cases, but with the default configuration an attack would take a long time to succeed.

- **Exim email servers are now under attack [7] [Ed: The drama queen that CBS hired (Cimpanu) says "Almost half of the internet's email servers are now being attacked with a new exploit." It sounds a lot worse when in fact many are patched and the "half" refers to number of installs, not attacks. Misreporting. FUD. ZDNet is not a news site but a tech tabloid. It should be regarded as such.]**

Security

Source URL: http://www.tuxmachines.org/node/124866

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/791052/rss
[3] https://www.kali.org/news/wsl2-and-kali/
[4] http://linuxgizmos.com/security-service-tracks-embedded-linux-vulnerabilities/
[5] https://nakedsecurity.sophos.com/2019/06/13/vim-devs-fix-system-pwning-text-editor-bug/
[6] https://www.itwire.com/security/mail-servers-running-exim-come-under-attack.html
[7] https://www.zdnet.com/article/exim-email-servers-are-now-under-attack/