Security updates have been issued by Debian (tomcat8), Fedora (chromium and okular), openSUSE (texlive-filesystem), Oracle (tomcat6), Scientific Linux (libvncserver, thunderbird, and tomcat6), Slackware (gd), SUSE (cloud-init, postgresql10, python36, and strongswan), and Ubuntu (ibus and vim).

Pwn2Own witnessed hackers defeating the security of not just Windows 10, but also macOS and Ubuntu all on the very first day.

Due to the coronavirus outbreak, the big hacking event was held with all those involved participating remotely with their exploits prepared in advance rather than in Vancouver as is usually the case (as part of the CanSecWest security conference).

We've already discussed the perils of code and composition scanning. If you've not already read those, you should go back to the beginning.

Now we're going to discuss application scanning. The basic idea here is we have a scanner that interacts with a running application and looks for bugs. The other two scanners run...
against static content. A running application is dynamic and ever changing. If we thought code
scanning was hard, this is even harder. Well it can be harder, it can also be easier. Sometimes.

Security

Source URL: http://www.tuxmachines.org/node/135582

Links:
[2] https://lwn.net/Articles/815882/rss