

Security: Small Airplanes, Hutchins, Updates, Windows XP and WireGuard

By *Roy Schestowitz*

Created 31/07/2019 - 7:18pm

Submitted by Roy Schestowitz on Wednesday 31st of July 2019 07:18:11 PM Filed under [Security](#) [1]

- [US issues hacking security alert for small planes](#) [2] [iophk: as planes become networked, attacks will no longer require physical access, such a thing has happened in cars.]

The cybersecurity firm, Rapid7, found that an attacker could potentially disrupt electronic messages transmitted across a small plane's network, for example by attaching a small device to its wiring, that would affect aircraft systems.

Engine readings, compass data, altitude and other readings ?could all be manipulated to provide false measurements to the pilot,? according to the DHS alert.

- [Small Airplanes Can Be Hacked to Display False Data in Flight](#) [3]

However, the [attack] requires physical access.

[...]

Rapid7 verified the findings by investigating two commercially available avionics systems. It determined that only "some level of physical access" to the aircraft's wiring was needed to pull off the hack, which could be delivered by attaching a small device to the plane's Controller Area Network (CAN) bus to send the false commands.

The key problem is that the CAN bus is integrated into the plane's other components without any firewalls or authentication systems in place. This means untrusted connections over a USB adapter hooked up to the plane can send commands to its electronic systems.

- [No Jail Time for ?WannaCry Hero? \[4\] \[iophk: the plea "bargain" still means he has become a convicted felon\]](#)

Hutchins' conviction means he will no longer be allowed to stay in or visit the United States, although Judge Stadtmeuller reportedly suggested Hutchins should seek a presidential pardon, which would enable him to return and work here.

- [Security updates for Wednesday \[5\]](#)

Security updates have been issued by CentOS (389-ds-base, curl, and kernel), Debian (libssh2), Fedora (kernel, kernel-headers, and oniguruma), openSUSE (chromium, openexr, thunderbird, and virtualbox), Oracle (389-ds-base, curl, httpd, kernel, and libssh2), Red Hat (nss and nspr and ruby:2.5), Scientific Linux (httpd and kernel), SUSE (java-1_8_0-openjdk, mariadb, mariadb-connector-c, polkit, and python-requests), and Ubuntu (openjdk-8, openldap, and sox).

- [It's 2019, and one third of businesses still have active Windows XP deployments \[6\] \[Ed: The problem is that they use Windows \(back doors in all versions\), not that they use "XP". They should move corporate data to something secure like BSD and GNU/Linux.\]](#)

Zero-day attacks were the second-most cited concern among IT decision makers, according to SpiceWorks, with 18% of respondents citing that as their primary concern. Insider data leaks were the most cited, at 27%, while attacks on IoT devices was third (17%), followed by supply-chain attacks (15%), DDoS attacks (15%), and cryptojacking (15%). Fewer than 20% of respondents indicated their business was "completely prepared" for common security threats.

Considering the risks that accompany unsupported software generally, and the larger attack surface that results from an unsupported (or otherwise unpatched) operating system, there is a relative lack of urgency to migrate from Windows 7. Certainly, while paid support for volume licenses is a possibility for some, smaller organizations ineligible for volume licensing will be left out in the cold. To date, Microsoft has shown no signs of wavering in their intent to grant a reprieve to the remaining users of Windows 7. Without a major shift, or a reprieve from Redmond, the prospect of unpatched, internet-connected systems is fertile ground for botnet creation.

- [NordLynx: NordVPN Builds New Tech Around WireGuard \[7\]](#)

Well known Panama-based VPN provider NordVPN has announced their NordLynx technology today that is based on the WireGuard protocol.

NordLynx is the company's new "fast and secure" VPN solution built atop WireGuard. The company describes WireGuard as a "radical change" and "a breath of fresh air in the industry."

[Security](#)

Source URL: <http://www.tuxmachines.org/node/126478>

Links:

- [1] <http://www.tuxmachines.org/taxonomy/term/59>
- [2] <https://www.apnews.com/6219f26c3ea145b6b29b5e69115504a9>
- [3] <https://www.pcmag.com/news/369845/small-airplanes-can-be-hacked-to-display-false-data-in-fligh>
- [4] <https://krebsonsecurity.com/2019/07/no-jail-time-for-wannacry-hero/>
- [5] <https://lwn.net/Articles/795007/rss>
- [6] <https://www.techrepublic.com/article/its-2019-and-one-third-of-businesses-still-have-active-windows-xp-deployments/>
- [7] https://www.phoronix.com/scan.php?page=news_item&px=NordLynx-WireGuard