Proprietary Software and Security

By Roy Schestowitz
Created 12/03/2021 - 6:31pm
Submitted by Roy Schestowitz on Friday 12th of March 2021 06:31:23 PM Filed under Security [1]


  Put enough cameras up and pretty soon they become tasty targets for malicious hackers.

- Apple sues 11-year veteran MacBook designer for allegedly stealing trade secrets for a journalist[3]

  According to Apple’s suit, Lancaster and his correspondent began communicating in 2018 about the possibility of obtaining information; the two then spent the next year in communication. Lancaster then reportedly contacted his correspondent in spring 2019, asking him to investigate rumors of a potential Apple product that could mean trouble for my startup.? The lawsuit also claims that Lancaster boasted to a third party shortly after that conversation that his media contact would be writing a story on his startup if it hit $1 million in funding.

- Apple sues former employee for allegedly leaking trade secrets to the media[4]

  The tech giant is taking on Simon Lancaster, who worked at Apple for 11 years before departing in 2019, in a suit filed in federal court in San Jose, Calif., alleging he committed trade secret misappropriation and breached his contract. The lawsuit was first reported by Apple Insider.

  In the lawsuit, Apple asserts that Lancaster, who worked as an advanced materials lead and product design architect, abused his position and trust within the company to systematically
disseminate Apple?s sensitive trade secret information in an effort to obtain personal benefits.

- **HSBC now offers Mac-friendly choice scheme** [5]

  It?s the latest example of increasing adoption of Apple?s hardware within employee-choice schemes, which has helped the company seize a 23% share of the US enterprise PC market.

- **Mac upgrade opened sshd to brute force password attacks** [6]

  Why would it matter if the sshd config got reverted? Simple: it's because the stock Mac sshd install includes password-based auth, and that means someone can brute-force their way onto your machine if they can connect to it on port 22 for long enough.

- **Microsoft-owned GitHub pulls PoC for Exchange Server flaws** [7]

  The code was published on Wednesday by a Vietnamese researcher Nguyen Jang, according to a report in The Record, a website owned by the CIA-backed threat intelligence firm Recorded Future.

  But hours later, GitHub took down the code. iTWire has asked the company why it did this.

  British security researcher Marcus Hutchins, the first to make mention of the PoC, said in a tweet that it did not work in its original state, but needed some tweaks.

- **The latest Windows 10 update could cause your printer to crash your PC** [8]

  The latest Windows update has been causing problems for some printer owners, according to a report from Windows Latest (via Gizmodo). Users are reporting that they?re getting a blue screen when they try to open the print dialogue from Notepad, Office, or other programs. (You know that annoyingly ambiguous error message that?s like ?Your PC ran into a problem and needs to restart?? It?s that one.)

- **Protecting the conversational systems from cyber attacks** [9]

  The chatbots are fast automating customer service. As of July 2020 (based on an Invespero
study), 67% of the customers used a chatbot. About 40% of the customers do not care if they are being served by a bot or a human being as long as they get their information. Millennials are more comfortable with texting than phone calls to traditional call centers.

More importantly, the automated interactive systems deployed by the businesses are becoming conversational, shedding the menu-driven, rule-based genesis of the IVR time. For example, popular chat apps (conversational) are doubling up as payment apps (rules-driven).

Security

Source URL: http://www.tuxmachines.org/node/148739

Links:
[6] https://rachelbythebay.com/w/2021/03/10/sealed/