SWCP Portal

January 2025

Is TP-Link Dangerous?

By Mark Costlow

Welcome to 2025! Political, economic, and technological uncertainty abound. The only sure bet is that 2025 will be a wild ride.

News broke in mid-December that the US Government is **considering a ban on the sale of all TP-Link devices**, citing national security risks.

TP-Link is a Chinese company that makes network equipment and smart home devices. SWCP has recommended TP-Link products in the past (Deco mesh WiFi systems for homes and Omada managed WiFi systems in campus deployments such as apartment complexes).

The company was founded in Shenzhen, China in the 1990s. Their popularity surged during the Covid lock downs as millions of people outfitted home offices. They grabbed market share by combining full-featured devices with low prices.

In recent years TP-Link has split into two companies, headquartered in Shenzhen, China and Irvine, California. Originally founded by two brothers, one of them, Zhao Jianjun, runs TP-Link USA in California. While TP-Link has marketing and R&D centers worldwide, all **products are manufactured in China, Vietnam, and Brazil**.

What Are the Claims?

In August 2024 the US House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (CCP) **said Chinese-made WiFi routers from TP-Link are a threat to national security** and urged the Commerce Department to investigate. They claimed the Chinese-made routers are susceptible to state-sponsored hackers planting malware, spyware, or back doors in the products. They cited concerns that to comply with draconian CCP laws, TP-Link would be forced to hand over sensitive US information to Chinese intelligence officials.

They claim that TP-Link SOHO (small-office / home-office) routers are used by CCP intelligence operators to perpetrate cyber attacks in the US, and have been used in a **hacking campaign that targeted government officials in Europe**.

The Commerce Department investigation is underway, as are probes by the Defense and Justice Departments. The threat to ban TP-Link sales in 2025 comes from the Commerce Department.

TP-Link's response is that their devices are among many brands used in these types of cyber attacks and that they are no more susceptible to security flaws than other consumer router companies. They also claim, "the Chinese government does not have access to and control over the design and production of our routers and other devices. TP-Link Systems is no longer affiliated with China-based TP-LINK Technologies, which sells exclusively in mainland China. Further, TP-Link Systems and its subsidiaries do not sell any products to customers in mainland China."

It is apparent that TP-Link has tried to separate its China and non-China operations, to the point of doubtlessly sacrificing many operational efficiencies to enforce the separation. However, one cannot help but question, if devices sold in the US are manufactured in China, how solid is the partition?

The answer to the question, "Why TP-Link and why now?" may be found in a blog **post from Microsoft in October**. Since August 2023, they have been tracking persistent "**password spray**" attacks from networks of compromised devices they have collectively dubbed "CovertNetwork-1658". They have observed the credentials stolen in these attacks being used by multiple Chinese "threat actors" (CyberSecurity-Speak for "bad guys"). The final link in this chain is that most of the devices in CovertNetwork-1658 are TP-Link SOHO routers.

According to the Wall Street Journal, **TP-Link routers make up 65%** of the home router market. So it would almost be surprising if a large portion of any collection like CovertNetwork-1658 was NOT comprised of mostly TP-Link devices. But it also implicates the devices has having poor security. If they were better, their fraction of CovertNetwork-1658 would be smaller than their market share, but in fact it is bigger.

How Bad Is It?

The bottom line is it is impossible to know. There are competing claims that likely all contain a degree of truth. **US lawmakers say**, "TP-Link's unusual degree of vulnerabilities and required compliance with [Chinese] law are in and of themselves disconcerting." **TP-Link says** they have, "a secure, vertically integrated and US-owned international supply chain" and "nearly all products sold in the United States are manufactured in Vietnam."

Given that we're not likely to get clarity from the mouthpieces at the tops of these organizations, lets consider the devices themselves. We haven't seen evidence that they are acting as malware or spyware reporting back to foreign intelligence agents on their own out of the box. What we have seen is devices being compromised after installation, and then used by the crooks who broke into them for such purposes.

Here are the important questions, in terms of deciding whether to continue using them, with answers following:

1. Are the devices using bad security practices?
2. If so, is it purposeful?
3. Is it worse than other vendors?
4. What are the alternatives?

1. Is It Bad Security?

Yes. The security is bad. They allow default passwords to be used, and ship with old software libraries which have known bugs which could be fixed. Patches have not come quickly, and many users never apply them.

2. Is It On Purpose?

Cyber Warfare among nation-states is a real thing, and it is likely that any government would like to have a few million consumer devices in their pocket, ready to be used as pawns in those battles.

Our own US intelligence services are known to **intercept networking hardware during shipping** from the factory, in order to surreptitiously add spyware before it gets to the customer. **Cisco has admitted** they sometimes ship enterprise routers to residential addresses to be stealthily picked up by their customers, to avoid NSA tampering.

3. Is It Worse Than Others?

No. The entire sector of low-cost SOHO routers **has been like this for years**. To keep prices low, they use open source libraries, but they tend to use old versions on under-powered processors and have never been good about providing updates and making it easy for users to find and install them. **Security researchers have warned** about this problem and been mostly ignored.

The problem is largely economic, and echoed throughout the Internet of Things (IoT) ecosystem. Devices are made and sold as cheaply as possible and treated like finished objects. No money is budgeted to maintain older versions of hardware that was sold years ago and will never generate new revenue for the company. To fix this problem, companies must recognize the true life-cycle of these devices and build ongoing software support into the initial cost. Many companies include the cost of eventual disposal or recycling into purchase prices, and this is just another element of that ethos.

4. What Are The Alternatives?

If you have TP-Link gear and are uncomfortable using it, here are the options:

Replace it with other gear. Finding replacements immune to these risks is not easy. So-called Enterprise hardware is typically (but not always!) better about security and providing regular software updates, but will cost significantly more.

Improve device security with this checklist**:**

- Change default passwords. Many device takeovers happen because the default password was never changed.
- Ensure the administration control panel can only be accessed from inside your network and not from the outside Internet.
- Learn how to check for software updates and apply them. If there's no automatic option, set a reminder to check for updates every 90 or 180 days. Set the reminders far enough apart that it is not a constant chore, and close enough that you won't run with unpatched bugs for too long.

Keep the hardware, but replace the software. **OpenWrt** is an Open Source alternative that can **run on many SOHO routers from TP-Link** and other vendors. It has good default security, readily available updates and patches, and a community maintaining it that doesn't need to make money from it.

OpenWrt does require a bit of tech prowess though. It is not as simple as downloading a software update or new app on your phone. And unfortunately it does not work on more specialized devices like the Deco mesh WiFi and CenturyLink DSL routers.

Conclusions and Predictions

Given what we know, should we continue buying TP-Link devices and using the ones we have?

For right now, there is likely no need for a radical change. If you have existing devices, the advice above will help to secure them. If you are buying a new one and you're uncomfortable with the potential lack of support that would follow a sales ban, you should pick a different vendor. Regardless of which vendor, the security advice above still stands.

Our prediction is that the government will come to an agreement with TP-Link that involves improving device security over the whole device life-cycle, and a ban will probably not happen. But we really won't know until the various investigations are completed. Politics will play a crucial role, and it's anybody's guess whether the new administration will push for or against this Chinese tech giant. Watching what happens with Tik Tok may give some clues.

If this threat of a ban results in long-term changes at TP-Link to improve security, then it will have served its purpose. If it causes other device makers to follow suit out of fear of sanctions then that is an added bonus.

Southwest Cyberport - swcp.com
New Mexico's Expert Internet Service Provider since 1994
505-232-7992 | Support: help@swcp.com
5021 Indian School NE, Ste. 600, Albuquerque, NM 87110
Click on bold blue type in browser for links.