Researchers: Chinese-made GPS tracker highly vulnerable

July 19 2022, by FRANK BAJAK

The U.S. Homeland Security Department headquarters in northwest Washington is pictured on Feb. 25, 2015. A popular Chinese-made automotive GPS tracker used by individuals, government agencies and companies in 169 countries has severe software vulnerabilities, posing a potential danger to life and limb, national security and supply chains, cybersecurity researchers said in a report released Tuesday, July 19, 2022, to coincide with an advisory from the U.S. Cybersecurity and Infrastructure Security Agency listing six vulnerabilities.

Credit: AP Photo/Manuel Balce Ceneta, File

A popular Chinese-made automotive GPS tracker used in 169 countries has severe software vulnerabilities, posing a potential danger to highway safety, national security and supply chains, cybersecurity researchers have found.

A report by the Boston cybersecurity firm BitSight says the flaws could let attackers remotely hijack device-equipped vehicles, cutting off fuel to them and otherwise seizing control while they travel.

The researchers say users should immediately disable the MV720 GPS tracker until a fix becomes available. The report was released Tuesday to coincide with an advisory from the U.S. Cybersecurity and Infrastructure Security Agency listing five vulnerabilities.

BitSight said it tried unsuccessfully for months—beginning in September, with CISA joining it in late April—to engage the manufacturer, Shenzen-based MiCODUS, in discussion addressing the vulnerabilities. The Associated Press telephoned and emailed the company but got no response. A person who answered a phone number listed on its website was unable to respond in English.

CISA said in a statement that it was not aware of "any active exploitation" of the vulnerabilities.

GPS trackers are used globally to monitor vehicle fleets—from trucks to school buses to military vehicles—and protect them against theft. In addition to collecting data on vehicle location, they typically also monitor other metrics, such as driver behavior and fuel usage. Via remote access, many are wired to cut off a vehicle's fuel or alarm, lock

or unlock its doors and more.

Using the MV720, which BitSight says costs less than $25 per unit, a malicious user could remotely cut off the fuel line of a vehicle in motion, know a vehicle's real-time location for espionage purposes or intercept and taint location or other data to sabotage operations, said the principal BitSight researcher on the project, Pedro Umbelino.

He said multiple malicious scenarios are possible: First responders' vehicles could be crippled, or a hacker could shut off an engine and demand a cryptocurrency ransom of victims to avoid calling a mechanic.

The main vulnerabilities: The device comes with a default password that more than 90% of users don't change, and there is second, obscure but hard-coded password that works for all devices, BitSight found. It also found security flaws in the software of the web server used to remotely manage the GPS devices.

The manufacturer, MiCODUS claims an installed base of 1.5 million devices across 420,000 customers, said BitSight. Its research found they included a Fortune 50 energy company and an aerospace company, a national military in South America and in eastern Europe, a nuclear power plant operator and a national law enforcement agency in western Europe. It did not name any of them. Countries with the most users included, by continent: Brazil, Mexico, Spain and Russia.

Richard Clarke, the former U.S. cybersecurity czar, called the insecure GPS device yet another example of a smart Chinese-made product "that is phoning home and could be used maliciously by the Chinese government."

While Clarke said he doubted the tracker was designed for that purpose, the danger is real because Chinese companies are obliged by law to

follow their government's orders—which is why Washington has been seeking to minimize Chinese components in U.S. telecoms networks and why some in Congress are pushing for a ban on U.S. government purchases of Chinese drones.

"You just wonder, how often are we going to find these things that are infrastructure—where there's a potential for Chinese abuse—and the users don't know?" said Clarke.