Critical flaws in GPS tracker enable “disastrous” and “life-threatening” hacks

reader comments

68 with 55 posters participating

Share this story

A security firm and the US government are advising the public to immediately stop using a popular GPS tracking device or to at least minimize exposure to it, citing a host of vulnerabilities that make it possible for hackers to remotely disable cars while they’re moving, track location histories, disarm alarms, and cut off fuel.

An assessment from security firm BitSight found six vulnerabilities in the Micodus MV720, a GPS tracker that sells for about $20 and is widely available. The researchers who performed the assessment believe the same critical

vulnerabilities are present in other Micodus tracker models. The China-based manufacturer says 1.5 million of its tracking devices are deployed across 420,000 customers. BitSight found the device in use in 169 countries, with customers including governments, militaries, law enforcement agencies, and aerospace, shipping, and manufacturing companies.

BitSight discovered what it said were six “severe” vulnerabilities in the device that allow for a host of possible attacks. One flaw is the use of unencrypted HTTP communications that makes it possible for remote hackers to conduct adversary-in-the-middle attacks that intercept or change requests sent between the mobile application and supporting servers. Other vulnerabilities include a flawed authentication mechanism in the mobile app that can allow attackers to access the hardcoded key for locking down the trackers and the ability to use a custom IP address that makes it possible for hackers to monitor and control all communications to and from the device.

The security firm said it first contacted Micodus in September to notify company officials of the vulnerabilities. BitSight and CISA finally went public with the findings on Tuesday after trying for months to privately engage with the manufacturer. As of the time of writing, all of the vulnerabilities remain unpatched and unmitigated.

“BitSight recommends that individuals and organizations currently using MiCODUS MV720 GPS tracking devices disable these devices until a fix is made available,” researchers wrote. “Organizations using any MiCODUS GPS tracker, regardless of the model, should be alerted to insecurity regarding its system architecture, which may place any device at risk.”

The US Cybersecurity and Infrastructure Security Administration is also warning about the risks posed by the

critical security bugs.

“Successful exploitation of these vulnerabilities could allow an attacker control over any MV720 GPS tracker, granting access to location, routes, fuel cutoff commands, and the disarming of various features (e.g., alarms),” agency officials wrote.

The vulnerabilities include one tracked as CVE-2022-2107, a hardcoded password that carries a severity rating of 9.8 out of a possible 10. Micodus trackers use it as a master password. Hackers who obtain this passcode can use it to log in to the web server, impersonate the legitimate user, and send commands to the tracker through SMS communications that appear to come from the GPS user’s mobile number. With this control, hackers can:

• Gain complete control of any GPS tracker
• Access location information, routes, geofences, and track locations in real time
• Cut off fuel to vehicles
• Disarm alarms and other features

A separate vulnerability, CVE-2022-2141, leads to a broken authentication state in the protocol the Micodus server and the GPS tracker use to communicate. Other vulnerabilities include a hardcoded password used by the Micodus server, a reflected cross-site scripting error in the Web server, and an insecure direct object reference in the Web server. The other tracking designations include CVE-2022-2199, CVE-2022-34150, CVE-2022-33944.

“The exploitation of these vulnerabilities could have disastrous and even life-threatening implications,” BitSight researchers wrote. “For example, an attacker could exploit some of the vulnerabilities to cut fuel to an entire fleet of commercial or emergency vehicles. Or, the attacker could leverage GPS information to monitor and abruptly stop vehicles

on dangerous highways. Attackers could choose to surreptitiously track individuals or demand ransom payments to return disabled vehicles to working condition. There are many possible scenarios which could result in loss of life, property damage, privacy intrusions, and threaten national security.”

Attempts to reach Micodus for comment were unsuccessful.

The BitSight warnings are important. Anyone using one of these devices should turn it off immediately, if possible, and consult with a trained security specialist before using it again.

https://arstechnica.com/?p=1867912