apnews.com

US issues hacking security alert for small planes | AP News

By TAMI ABDOLLAH

6–8 minutes

WASHINGTON (AP) — The Department of Homeland Security issued a security alert Tuesday for small planes, warning that modern flight systems are vulnerable to hacking if someone manages to gain physical access to the aircraft.

An alert from the DHS critical infrastructure computer emergency response team recommends that plane owners ensure they restrict unauthorized physical access to their aircraft until the industry develops safeguards to address the issue, which was discovered by a Boston-based cybersecurity company and reported to the federal government.

Most airports have security in place to restrict unauthorized access and there is no evidence that anyone has exploited the vulnerability. But a DHS official told The Associated Press that the agency independently confirmed the security flaw with outside partners and a national research laboratory, and decided it was necessary to issue the warning.

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.

The warning reflects the fact that aircraft systems are increasingly reliant on networked communications systems, much like modern cars. The auto industry has already taken steps to address similar concerns after researchers exposed vulnerabilities.

The Rapid7 report focused only on small aircraft because their systems are easier for researchers to acquire. Large aircraft frequently use more complex systems and must meet additional security requirements. The DHS alert does not apply to older small planes with mechanical control systems.

But Patrick Kiley, Rapid7's lead researcher on the issue, said an attacker could exploit the vulnerability with access to a plane or by bypassing airport security.

"Someone with five minutes and a set of lock picks can gain access (or) there's easily access through the engine compartment," Kiley said.

Jeffrey Troy, president of the Aviation Information Sharing and Analysis Center, an industry organization for cybersecurity information, said there is a need to improve the security in networked operating systems but emphasized that the hack depends on bypassing physical security controls mandated by law.

With access, "you have hundreds of possibilities to disrupt any system or part of an aircraft," Troy said.

The Federal Aviation Administration said in a statement that a scenario where someone has unrestricted physical access is unlikely, but the report is also “an important reminder to remain vigilant” about physical and cybersecurity aircraft procedures.

Aviation cybersecurity has been an issue of growing concern around the world.

In March, the U.S. Department of Transportation’s inspector general found that the FAA had “not completed a comprehensive, strategy policy framework to identify and mitigate cybersecurity risks.” The FAA agreed and said it would look to have a plan in place by the end of September.

The UN’s body for aviation proposed its first strategy for securing civil aviation from hackers that’s expected to go before the General Assembly in September, said Pete Cooper, an ex-Royal Air Force fast jet pilot and cyber operations officer who advises the aviation industry.

The vulnerability disclosure report is the product of nearly two years of work by Rapid7. After their researchers assessed the flaw, the company alerted DHS. Tuesday’s DHS alert recommends manufacturers review how they implement these open electronics systems known as “the CAN bus” to limit a hacker’s ability to perform such an attack.

The CAN bus functions like a small plane’s central nervous system. Targeting it could allow an attacker to stealthily hijack a pilot’s instrument readings or even take control of the plane, according to the Rapid7 report obtained by The AP.

“CAN bus is completely insecure,” said Chris King, a cybersecurity

expert who has worked on vulnerability analysis of large-scale systems. “It was never designed to be in an adversarial environment, (so there’s) no validation” that what the system is being told to do is coming from a legitimate source.

Only a few years ago, most auto manufacturers used the open CAN bus system in their cars. But after researchers publicly demonstrated how they could be hacked, auto manufacturers added on layers of security, like putting critical functions on separate networks that are harder to access externally.

The disclosure highlights issues in the automotive and aviation industries about whether a software vulnerability should be treated like a safety defect — with its potential for costly manufacturer recalls and implied liability — and what responsibility manufacturers should have in ensuring their products are hardened against such attacks. The vulnerability also highlights the reality that it’s becoming increasingly difficult to separate cybersecurity from security overall.

“A lot of aviation folks don’t see the overlap between information security, cybersecurity, of an aircraft, and safety,” said Beau Woods, a cyber safety innovation fellow with the Atlantic Council, a Washington think tank. “They see them as distinct things.”

The CAN bus networking scheme was developed in the 1980s and is extremely popular for use in boats, drones, spacecraft, planes and cars — all areas where there’s more noise interference and it’s advantageous to have less wiring. It’s actually increasingly used in airplanes today due to the ease and cost of implementation, Kiley said.

Given that airplanes have a longer manufacturing cycle, “what we’re trying to do is get out ahead of this.”

The report didn’t name the vendors Rapid7 tested, but the company alerted them over a year ago, the report states.

———

Follow Tami Abdollah on Twitter at https://twitter.com/latams