Panasonic

December 20, 2016
Panasonic Avionics Corporation
26200 Enterprise Way
Lake Forest, CA 92630

Subject: IOActive Blog published by Ruben Santamarta

To Whom It May Concern:

The allegations made to the press by IOActive regarding in-flight entertainment (IFE) systems manufactured by Panasonic Avionics Corporation ("Panasonic") contain a number of inaccurate and misleading statements about Panasonic's systems. These misstatements and inaccuracies call into question many of the assertions made by IOActive.

Most notably, IOActive has chosen to make highly misleading and inflammatory statements suggesting that hackers could "theoretically" gain access to flight controls by hacking into Panasonic's IFE systems. Panasonic strenuously disagrees with any suggestion by IOActive that such an attack is possible, and calls upon IOActive to clarify that its research does not support any such inference.

IOActive has presented no evidence that its examination of Panasonic's systems would support any such suggestion, and its statement that its "research revealed it would also theoretically be possible that such a vulnerability could present an entry point to the wider network, including the aircraft controls domain" will only serve to falsely alarm the flying public.

Furthermore, IOActive employee Ruben Santamarta's statement regarding credit card theft is simply not true. Mr. Santamarta makes incorrect assumptions about where credit card data is stored and encrypted within Panasonic's systems.

It is important to note that, during the course of this unauthorized, in-service testing, the safety, security and comfort of passengers of the aircraft were never in danger or compromised due to the system segregation and robust security design of our inflight entertainment and communications (IFEC) product, and of all commercial aircraft as well. His exploit itself was limited to a single seat and information gathering; control override of the IFEC seat and system did not occur.

It is also very important to note that, in its communications to the press, IOActive made unfounded, unproven conclusions. The basis for many of these conclusions would first necessitate that an attacker gained a physical connection within the IFE network.

During the unauthorized testing, network penetration, or even network connection to Pansonic's product, did not occur.

The conclusions suggested by IOActive to the press are not based on any actual findings or facts. The implied potential impacts should be interpreted as theoretical at best, sensationalizing at worst, and absolutely not justified by any hypothetical vulnerability findings discovered by IOActive.

IOActive, in statements to the press, inappropriately mixed a discussion of hypothetical vulnerabilities inherent to all aircraft electronics systems with specific findings regarding Panasonic's systems, creating a highly misleading impression that Panasonic's systems have been found to be a source of insecurity to aircraft operation.

Like any responsible business, Panasonic continually tests the robustness of its systems, and reviewed all of the claims made by Mr. Santamarta. It subsequently engaged Attack Research (AR) to conduct validation testing in May 2015 and again in 2016 to ensure that the few minor concerns (in no way linked to the control of an aircraft) identified by Mr. Santamarta had been fully remediated, and this was confirmed in a written report to Panasonic.

Panasonic does not condone unauthorized security testing during aircraft operation in uncontrolled environments, such as those conducted by IOActive. Panasonic strongly supports legislation that should be enacted to make on-board electronic intrusion a criminal act.

Security professionals who wish to test our systems legitimately and safely can do so by participating in our Bug Bounty program (bugbounty@panasonic.aero) in which Panasonic provides unfettered access to our products to allow for in-depth security testing and analysis.

Panasonic IFE products have a robust security design that complies with, or exceeds, all requirements, and are routinely and regularly tested by third-party professional security firms, as well as by participants in our independent Bug Bounty program.

Panasonic also fully supports aircraft manufacturers and aviation regulatory agencies to ensure our IFE systems are designed to comply with all aircraft manufacturer and regulatory security requirements, and Panasonic routinely reviews our designs with said groups.

Additionally, Panasonic is a member of the Aviation Information Sharing and Analysis Center (A-ISAC) for the express purpose of assuring that vulnerabilities are shared

and assessed with a collective oversight so that the integrity of the systems can be maintained. Panasonic's IFE software is certified at Level-E per DO-178B, with "No Effect" to aircraft safety.

Sincerely,
Panasonic Avionics Corporation

CONTACT:
Brian Bardwell
Corporate Communications Manager
Panasonic Avionics Corporation
Brian.Bardwell@panasonic.aero