IOActive has a stringent and thorough process by which it technically validates published research and the company stands by the accuracy and integrity of the findings with regard to the research recently published on Panasonic Avionics IFE systems.

As with virtually all security-related research, the findings are made up of both documented technical findings regarding the vulnerabilities described, as well as statements of opinion, theory and/or feasibility by the researcher that were developed based on both the merits of the technical findings, as well as the researcher's vast domain expertise, experience, and knowledge on the subject matter presented – as evidenced by current and past research published.

While we cannot control how the information presented is precisely interpreted, represented, or disseminated across all outlets, we have absolute confidence in the accuracy of the technical findings and the merit of observations and opinions contained in the research documentation, including the technical feasibility of the theoretical references. In some cases, direct access to files and systems is no longer available to extend the research and validate or discount the actual feasibility of things such as the IFE system being used as an entry point to other systems not detailed in the research. Additionally, some of the opinions and references to theoretical scenarios referenced in the research have little or nothing to do with the IFE system itself and more to do with the configuration, or potential misconfiguration, of other systems inherent in an airplane's IT ecosystem.

Quite simply, if an attacker is able to exploit vulnerabilities acknowledged to be resident (and claimed to be subsequently addressed) by the manufacturer in a technology component within a connected ecosystem (i.e., say an IFE on board a plane), and the ecosystem is not configured appropriately to segment and isolate the respective domains as they should be, then exploiting the vulnerabilities in that component to gain access to other domains in the ecosystem is technically feasible and "theoretically" quite possible. So not only are the theoretical statements in the research technically feasible and relevant to the topic of the research, but they are important in explaining the potential extent and possible implications of vulnerabilities within a component in such an ecosystem and the need for a holistic approach to managing and maintaining the highest security measures at all levels throughout that ecosystem.

It's about raising valid security awareness and while it's unfortunate that pieces of the work are taken out of context and used to sensationalize the research in some outlets to get clicks, the original research, vulnerabilities disclosed, and statements of technical feasibility – theoretical or otherwise – are absolutely spot on and we will stand by and further detail/defend them as/if needed.

Finally, it should also be noted that the manufacturer's public statement on the matter includes references and statements that are not included within IOActive's published documentation on this research (i.e., the blog post and press release appearing on the IOActive website). The content published on our site within both documents is accurate based on the research findings.

We believe that it is in the long-term best interests of the public, the aviation industry, aviation product security teams, and the manufacturer in this case to publicly disclose this example of cybersecurity risk in the aviation industry. Our intent with publicly describing these vulnerabilities is to create informed, fact-based public awareness about the presence of cybersecurity risks in aviation and demonstrate the risks in a responsible manner to ensure that senior management and stakeholders within the aviation industry allocate appropriate levels of resources to deal with these risks.