Analysis of AirVision / AV-Trend / Model 8872 and Spectre/Meltdown Vulnerabilities

Agilaire's analysis regarding the Spectre and Meltdown vulnerabilities indicate no unique vulnerability in our AirVision/AV-Trend software or the 8872 platform, other than known vulnerabilities within the Windows OS and default or user-installed browsers.

Industry articles indicate the two primary vectors of attack are:

1. A malicious program installed on the computer
2. Connecting to a web site hosting malicious javascript code

With regards to Vector 1, the primary defense should be standard anti-virus software, like the built-in Windows Defender, or other third party programs used by the customer. This vector is unlikely, as a malicious program that makes its way past anti-virus defenses could have more direct methods of attack (e.g., keyloggers), and that using the Spectre/Meltdown vulnerability is a less efficient way of compromising a system.

With regards to Vector 2, the standard AirVision and Model 8872 deployment does not use any browser interfaces, and the dedicated client system used does not offer any opportunity to view or report on kernel or system memory.

The Model 8872 does offer a web service interface for its TechAssist app, and the AirVision system does offer a web AQS service for the Exchange Network plugins. These web services offer a very limited interface of available data (again, no kernel or system memory dump options programmed specifically into the interface), and use the standard Microsoft .NET WebAPI, so it is assumed Microsoft would address vulnerabilities within the .NET framework.

Finally, our application does include a 'crash report' that includes some system information (OS versions, .NET version, etc), but we have reviewed and found no information in the report related to either of these exploits.

In conclusion, we see no vulnerability in our products other than standard Windows OS vulnerabilities. We recommend:

- using the built-in Windows Defender (or other antivirus program) with any real-time file scanning processes set to exclude the SQL / SQLExpress database files for AVData
- keeping up with important/critical (NOT optional) Windows Updates
- keeping web browsers up to date