vaddio | THE ART OF EASY BULLETIN

Minimal Malware Risk to Vaddio Products

What we have learned about the Spectre and Meltdown Vulnerabilities:

Vaddio customers have expressed an understandable level of concern about the Spectre and Meltdown vulnerabilities. We are committed to keeping your Vaddio products secure.

We are still investigating the Spectre and Meltdown vulnerabilities. To date, this is what we have learned:

- *According to malware researchers, Meltdown and Spectre can only be exploited with malicious code that is present and running on the device.* Vaddio products' firmware is encrypted, disallowing the installation of malicious code on the device.
- *The Spectre and Meltdown vulnerabilities do not allow remote code execution.* Your Vaddio equipment cannot be used as a route to spread malware through your network.
- *The Spectre and Meltdown vulnerabilities only enable a third party to read device memory locations actively being used by other parts of the device software.* Although PCs and other computing devices store a great deal of sensitive data, Vaddio products do not contain this type of data, nor do they provide a route to access sensitive data elsewhere on your network.

Where appropriate, Vaddio's Software Engineering team expects to include a patch for these vulnerabilities as part of normal system updates going forward.

.