“Spectre” and “Meltdown” Attacks

There has been a lot of recent discussion of the “Spectre” and “Meltdown” attacks and how they can affect the security of a system. Both attacks take advantage of the fact that modern, high-speed processors execute instructions speculatively i.e. they assume that, for example, a given condition will be true and execute instructions accordingly. If it later turns out that the condition was false, the speculatively executed instructions are discarded as if they had no effect.

The embedded processors within Finisar’s WaveShaper and WaveAnalyzer products do NOT use speculative execution and so are immune from attack using the techniques described in the “Spectre” and “Meltdown” attacks.

We do, however, recommend that any computer which is used to control a WaveShaper or WaveAnalyzer be regularly updated with any recommended patches from the manufacturers of the hardware, operating system (Windows/Linux/MacOS) or browser implemented when available to minimise the potential for attack.

Ceramics & Composites

Rare Metals

Global Sales Network

Legal I Privacy I Cookies

Legal I Privacy I Cookies

© 2024 Coherent Corp.

Cookie Preferences