

BEC Technologies Security Update: Meltdown and Spectre

BEC is fully aware of the [Spectre](#) and [Meltdown](#) vulnerabilities that were recently reported by numbers of security researchers. For BEC products, we do not use Intel, AMD, or ARM processors, and as a consequence, the Meltdown and Spectre do not affect any BEC routers.

Spectre and Meltdown vulnerabilities impact the confidentiality of data running on Intel, AMD and ARM processors. The Meltdown and Spectre flaws—two related vulnerabilities that enable a wide range of information disclosure from every mainstream processor, with particularly severe flaws for Intel, AMD, and some ARM chips. Meltdown attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system. Spectre allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. Technical details on the vulnerabilities can be found on the dedicated site meltdownattack.com. The related CVEs are shown below:

CVE-2017-5715
CVE-2017-5753
CVE-2017-5754

Further Updates:

Additional information will be provided as soon as it is available. (Jan. 10th, 2018)