The CYBER GURU

Ali Maroufi
Cybersecurity Officer

Severe design flaws in modern central processing units (CPUs), including Intel, Qualcomm, AMD, and ARM processers were recently disclosed, triggering a wave of urgent security advisories and patches.

The problem lies in the way these processors have been designed to rely on a technique called speculative execution to optimize performance. Optimization is done by predicting the instructions they are going to be executing next.

Exploiting these vulnerabilities – known as Meltdown and Spectre – is very challenging. In some attacks, physical access is required. This means that a hacker has to spend a lot of time and effort to access an average user's machine where it would be much easier to get the access via phishing. On the other hand, for high-value targets like financial and educational institutions, Meltdown and Spectre vulnerabilities are a cause to be concerned.

Companies are working to apply available patches while dealing with the performance hit caused by these patches. The average user should not see a major performance changes from these vulnerabilities. Those using process-intensive tasks like video editing and some gaming programs will notice the slowdown.