WIND

AN INTEL COMPANY

SPECTRE AND MELTDOWN FAQ

CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754, also referred to as Spectre and Meltdown, are security vulnerabilities that potentially allow for the gathering of sensitive data improperly from computing devices.

These exploits are based on side-channel analysis. A side-channel is some observable aspect of a computer system's physical operation, such as timing, power consumption or even sound. The statistical analysis of these behaviors can in some cases be used to potentially expose sensitive data on computer systems that are operating as designed. These exploits do not have the potential to corrupt, modify or delete data. All of the methods take advantage of speculative execution, a common technique in processors used to achieve high performance

- **Is my product impacted?**
- **How do I determine whether the prerequisites are met?**
- **Is this a bug in Wind River software?**
- **What solutions will Wind River products provide?**
- **Why do Wind River solutions differ between processors within a product version?**
- **Why do Wind River solutions differ between products?**
- **What is the time table for Wind River solutions?**
- **How will Wind River incorporate support for processor microcode updates as they become available?**

1. **Q: Is my product impacted?**

   A: For a product to be vulnerable to Spectre or Meltdown, or both, four prerequisites must be in place:

   - The processor must implement features that can be exploited by Spectre or Meltdown
   - The attacker must have an available timing source granular enough to measure the impacts of speculative execution
   - The attacker must be able to run attack code on the processor
   - There must be information accessible to the processor that an attacker is not authorized to access

   If all four prerequisites are met, then the product is potentially vulnerable to one or more of the Spectre and Meltdown exploits.

2. **Q: How do I determine whether the prerequisites are met?**

   - A: The processor must implement features that can be exploited by Spectre or Meltdown
     - Determine whether your processor is vulnerable to Spectre, Meltdown, or both using the processor vendor's guidance and documentation

- The attacker must have an available timing source granular enough to measure the impacts of speculative execution
  - This can be somewhat system dependent, but in general if only coarse grain timers are available (i.e., smallest timing measurement is on the order of 1000 processor clock cycles or more), exploiting timing of speculative execution is extremely challenging
- The attacker must be able to run attack code on the processor
  - Spectre and Meltdown are not remote attacks, they require attacker code to be running on the processor and measuring the timing of speculative execution. Many embedded systems or mission critical systems are highly constrained and only allow a prescribed, pre-defined, and verified set of functions to run on the system. In these types of systems, for example, the likelihood of an attacker running attack code on the processor may be low enough that the risk is acceptable
- There must be information accessible to the processor that the attacker is not authorized to access
  - The Spectre and Meltdown issues do not have the potential to corrupt, modify, or delete data, so if the system does not contain information that an attacker is not authorized to access, there would be no impact related to a successful attack and the risk may be acceptable. For example, in platforms that do not implement separation between privilege modes (e.g., kernel vs. userspace), any code running on the processor is authorized to access any data available to the processor

If the prerequisites are met, and it is determined that the product is potentially vulnerable to one or more of the Spectre and Meltdown exploits, Wind River encourages our customers to take a risk-based approach to determining the appropriate solutions for their system. These solutions may include the processor vendor recommended mitigations, and/or other alternatives that mitigate the risk associated with Spectre and Meltdown exploits. Examples of alternative mitigations include:

- Integration of secure boot and transition to a closed environment that prevents attackers from being able to run exploit code on the processor
- Storage of, and operation on, information that needs to be protected in a hard ware security module such as a TPM so that sensitive information is not available in processor memory where it could be disclosed through a Meltdown or Spectre exploit

3. Q: Is this a bug in Wind River software?

A: No. This is not a bug or a flaw in Wind River products. These new exploits leverage data regarding the proper operation of processing techniques common to modern computing platforms, potentially compromising security even though a system is operating exactly as it is designed to. Updates to Wind River products provide software-based mitigation solutions to these exploits and are aligned with mitigations recommended by the processor suppliers.

4. **Q: What solutions will Wind River products provide?**

   A: Wind River will provide up-to-date mitigation solutions for currently supported products that are impacted by affected processors. See Wind River's security page for the current list here: http://www.windriver.com/security/announcements/meltdown-spectre/.

   The most effective mitigation solution to Spectre and Meltdown exploits will vary by variant, processor, and Wind River operating system, and may include updates to the operating system and firmware. Wind River will provide updates based on software mitigations recommended by the processor suppliers. See the Wind River Knowledge Base security alerts at https://knowledge.windriver.com for Spectre and Meltdown CVEs (CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754) for more information.

   In the markets Wind River serves, our customers may determine that system tradeoffs dictate the use of alternative solutions based on a variety of factors such as risk, safety, cost, etc. Security solutions available in Wind River products, including secure boot and hardware security module support, may mitigate the risk sufficiently in some cases. We encourage our customers to take a risk based approach to determining the appropriate solutions for their system.

5. **Q: Why do Wind River solutions differ between processors within a product version?**

   A: Within a specific version of a Wind River product, solutions may differ by processor because the Spectre and Meltdown variants affect processors differently. In addition, the specific mitigations for the same variant may differ by processor (e.g., processors vary in mechanisms to prevent branch speculation).

6. **Q: Why do Wind River solutions differ between products?**

   A: Solutions may differ because, depending on the use case, Wind River products could leverage the underlying processor mechanisms differently and some products may leverage those mechanisms in ways that are potentially exploitable, whereas other products do not.

7. **Q: What is the time table for Wind River solutions?**

   A: Initial solutions for Wind River products will start becoming available by late January 2018. In most cases, solutions for the most recent product versions will be available first and will be followed by solutions for older versions. Additionally, solutions for the full set of supported processors for each product will be added over time. This is primarily due to two factors: availability of processor vendor solution recommendations, and availability of robust, mature implementations of those solutions.

   For more information about the availability of solutions for the Wind River product version and processor combination, please see the product's security alert available on Wind River's support site (https://knowledge.windriver.com). Links to security alerts for each currently supported Wind River product can be found on our Meltdown and Spectre security announcement here: http://www.windriver.com/security/announcements/meltdown-spectre/.

8. **Q: How will Wind River incorporate support for processor microcode updates as they become available?**

   A: Microcode updates for processors can be applied in multiple parts of the system, from processor firmware to operating system. In some of Wind River's operating system products, we provide microcode patches that apply processor vendor supplied microcode updates from the operating system. These microcode patches are available on our support site and are downloadable as part of product maintenance.

   In some cases, solutions require combined microcode and companion operating system updates that leverage features of the updated microcode. In these cases, Wind River product updates, made available through our product maintenance tools, will contain both the microcode updates and Wind River product updates. All updates will be announced in the product release information available on Wind River's product support site - https://knowledge.windriver.com.

8. **Q: Will applying updates to address this issue hurt the performance of my system?**

   A: Ultimately, overall impact will depend on the specific workload, platform configuration and mitigation technique. In some cases there are multiple mitigation options available, each with different performance implications and implementation specifics.

   Multiple sources, including processor vendors, have begun to share performance results and we encourage our customers to evaluate information from those sources in the context of specific characteristics of the workloads on their system.

REFERENCES

1. https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html
2. https://newsroom.intel.com/news/intel-offers-security-issue-update/
3. https://newsroom.intel.com/news-releases/industry-testing-shows-recently-released-security-updates-not-impacting-performance-real-world-deployments/

WIND
AN INTEL COMPANY