January 10th, 2018

Advantech Product Security Bulletin
Meltdown and Spectre Side-Channel Vulnerability

CPU hardware implementations are vulnerable to side-channel attacks referred to as Meltdown and Spectre. Exploitation of these vulnerabilities could allow an attacker to obtain access to sensitive information. The information in this Security Bulletin should be acted upon as soon as possible.

■ Overview:

There is an escalation of security vulnerability in systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. Security researchers disclosed several software analysis methods that, when used for malicious purposes, have the potential to improperly gather sensitive data from many types of computing devices with many different vendors' processors and operating systems.

■ References:

1. US-CERT:
   https://www.us-cert.gov/ncas/alerts/TA18-004A

2. Intel Security Center (INTEL-SA-00088):
   https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

3. AMD Processor Security Announcement:
   https://www.amd.com/en/corporate/speculative-execution

4. ARM Processor Security Announcement:
   https://developer.arm.com/support/security-update

5. Microsoft Security Center:
   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

6. Android Security Bulletin:
   https://source.android.com/security/bulletin/2018-01-01

7. Linux Security Center:
   https://lkml.org/lkml/2017/12/4/709

■ Description:

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs.

Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.

Meltdown:

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

Spectre:

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre. Spectre is harder to exploit than Meltdown, but it is also harder to mitigate.

The difference between Meltdown and Spectre:

Meltdown breaks the mechanism that keeps applications from accessing arbitrary system memory. Consequently, applications can access system memory. Spectre tricks other applications into accessing arbitrary locations in their memory. Both attacks use side channels to obtain the information from the accessed memory location.

Impact:

For the affected microprocessor vendor and part number list, please refer to the US CERT website above first. Exploitation of these vulnerabilities could allow an attacker to obtain access to sensitive information. It will affect the safety aspect of product application, there is no practical customer security case take place up to now. Any malware using this side channel analysis method must be running locally on the machine. Following good security practices that protect against malware in general will also help to protect against possible exploitation until updates can be applied.

Recommendation:

(1) Protect your Administrator Privileges:

Advantech strongly encourage customers to consistently undertake safe computing practices, following good security practices protect against malware in general will also help to protect against possible exploitation of these analysis methods. Some of these include:

- Maintain control of your computing environment
- Regularly check for and apply available firmware/driver updates
- Use hardware and software firewalls
- Turn off unused services
- Maintain appropriate user privileges
- Keep security software up to date
- Avoid clicking on unknown links
- Avoid re-using passwords across sites
- Follow strong password protocols
- Not installing the unknown software/programs

(2) There are two corrective actions needed for solving the Meltdown and Spectre hazards:

- Operating System update:

  Advantech encourage customers to update the Operating System(OS) patches, refer to the OS vendors for the most recent information. The table provided in the Operating System Vendor Information List below (source from US CERT) for the available advisories and OS updated patches.

Source: From US CERT website (Operating System Vendor Information List)
https://www.us-cert.gov/ncas/alerts/TA18-004A

Vendor Information List
Android
Apple
CentOS
Linux
Microsoft

- Microprocessor vendor micro-code update:
  The microprocessor vendors are updating the micro-code patch solutions to solve these security risks, there are still issues to be solved by Intel for further investigation. Advantech will continuously to pull-in the schedule for updating.

Thank you for choosing Advantech products, and we appreciate you are Advantech's valuable customer.

Sincerely,

YS. Yang

Advantech
Corporate Quality