TÜVRheinland®
Precisely Right.

TÜV Rheinland – Security Advice – Meltdown & Spectre – January 08, 2018

Massive security vulnerabilities discovered in processors – What to do now to avoid being a victim

What happened?

An international team of security researchers has discovered serious security vulnerabilities in CPUs. The processor vulnerabilities potentially allow attackers to gain access to sensitive data such as passwords, user data or confidential information.

What is it affecting?

Most processors that are built into computers from servers to desktop PCs as well as mobile devices such as laptops, smartphones and tablets are affected. The vulnerabilities are found in many makes of processors including those used in Apple devices. A number of security updates have already been released.

Why is the problem so massive?

The vulnerabilities are due to a major design flaw in computer processors. Thus far, a specific attack using this flaw is yet to be seen in public, but it is only a matter of time until bad actors take advantage of it. The sheer number of affected devices is so great that it will prove a very tempting attack vector whilst systems go through appropriate remediation steps. Quantitatively, billions of devices are probably impacted.

What exactly is the problem?

In order to improve performance, computer processors may speculatively execute code or take steps to prepare data to be processed ahead of being requested by the user. During this preparation phase, access rights are not always checked, providing a gap in the processor security model that could be exploited by an attacker.

There have been two bugs identified;

- **Meltdown** allows data to be accessed on a processor in areas normally inaccessible to normal user software. By accessing this area, a computer's physical memory could be examined and data – including passwords and intellectual property such as process control data or plant administrators' credentials – exfiltrated.

- **Spectre** allows certain types of programs operating in what is called user mode to extract data from other processes on the same system. This bug is not easy to patch and requires software to be recompiled with countermeasures to provide protection.

Characteristics and Threats for Shared Hosting environments

Based on the information provided by ARM, Intel and Google, Meltdown/Spectre threatens confidentiality of data on systems where malicious entities can execute their code locally. This may limit to some extent the attack vector as an attacker must have privileges to run his code on the machine in order to threaten confidentiality.

Most important to note is that the ability to read data from memory is not limited to the virtual machine an attacker has access to but also to the memory of the underlying physical machine. In shared hosting environments such as AWS, Google Cloud Platform and Azure, this becomes a real threat as often different companies and users may share one physical machine. In such a case, a user might have access to another user's data that is stored in the memory of the same physical machine.

Threats for Clients

Meltdown/Spectre can also impact client PCs as a user may be able to read data to which he normally has no access to. This can lead to a privilege escalation on a machine, e.g., a user may be able to read an NTLM hash in machine memory. Smartphones could be compromised by a malicious app that facilitates data access using Meltdown or Spectre.

Impact on IoT devices

For IoT devices, it is seldom the case that an attacker can run his code on the system in the first place. In addition, most IoT devices use simpler CPUs that are not affected by Meltdown/Spectre. So the attack vector is quite limited.

Processors in typical IoT devices are probably not going to be affected for two reasons.

- Speculative execution, which causes the problem, is not needed because the computing power is sufficient for many IoT devices without this feature.
- Speculative execution adversely impacts power consumption as instructions are executed that may not have been needed. IoT devices often have a very limited power budget that precludes such processing.

What should you do to protect your organization?

To prevent becoming a victim of the current Meltdown or Spectre vulnerabilities, companies, especially industrial systems operators, should consider the following steps:

1. Don't panic. There are potentially other, less sophisticated ways in which an attacker could compromise your plant or operation, so you probably have time to address this issue.
2. Immediately start patching your devices. Performance impact of patching: Current estimates of performance impact of the patches range between 5% and 40% from researchers testing patches in labs. The operating system patches avoid using performance features where vulnerabilities lie.

3. Review your OT estate or control systems and determine if it may be impacted by these issues. Note that the Meltdown bug reportedly impacts all out-of-order execution Intel processors since 1995, including out-of-order x86-64 Intel CPUs available since 2011. Check your process control hardware and speak with your system vendors and see if they have issued an alert, advisory or patch.

4. Take a risk based approach to applying any software updates or patches to your plant equipment. Windows and Linux patches are available now for the Meltdown bug, but the Spectre bug is currently not patchable. Hopefully, you have a patch management policy in place that enables you to evaluate reported issues and make a determination as to whether a patch needs to be applied immediately or can be scheduled for a later time.

5. Think about your ERP or IT systems that may be impacted and ensure that your IT department has patched or has a plan in place to patch affected systems.

6. Security Analytics should be tuned to look for geographical anomalies in logins as well as coordination with DLP sensors (Data Leakage Prevention). Monitor your systems for abnormal behavior (Indicators of Compromise).

7. Having a good defense-in-depth strategy in place also helps to minimize the risk that Meltdown/Spectre represents for an environment. This includes but is not limited to:
   a. Having different security zones that do not overlap.
   b. Virtualize only systems on the same physical host that process similar data regarding its CIA (confidentiality, integrity, availability) requirements.
   c. Do not virtualize systems hosting highly critical data, e.g., central authentication systems.
   d. Do not reuse password/credentials in a different security zone (or security tiers).
   e. Patch your systems regularly.
   f. Have a proper and mature vulnerability management process in place that covers all components starting for servers, network components, software library, firmware, etc.
   g. Carefully select your third party service providers.

8. Take this as an opportunity to review your overall operational technology cybersecurity risk and make sure that you have implemented good processes, policies and controls to manage this in a proportionate way. Consider an OT threat monitoring solution that could help monitor for such issues in the future.

Maybe a victim already – what then?

If you suspect that you have already been attacked, you should contact a trusted Cyber Security Affiliate to provide you with the help you need, investigate further and limit the damage.

You need help?

For immediate assistance, please contact one of your regional cyber security partners:

North America
Mitch Lapidus
Vice President of Sales, OpenSky Corp, TÜV Rheinland Company
Tel: +1 (973) 479-7457
Email: MLapidus@openskycorp.com

Europe (West, East, and Central)
Bjoern Haan
Regional Field Manager Cyber Security, TÜV Rheinland i-sec GmbH
Tel: +49 174 1880240
Email: Bjoern.Haan@i-sec.tuv.com

Middle East, Africa, Asia Pacific
John Ramesh
Managing Director, TUV Rheinland L.L.C, Oman
Tel: +968 9423 4267
Email: john.ramesh@om.tuv.com

Asia Pacific, Japan & China
Sandeep Sinha Roy
Vice President of Sales, ICT & BS, TÜV Rheinland Singapore Pte. Ltd., Singapore
Tel: +65 6562 8750 ext 3323
Email: sandeep.sinharoy@tuv.com