INTECH COMPUTER SOLUTIONS
Intelligent
Integrity.
In time.

Tallis Newkirk
tallis@intechcs.ca
306.914.0846

integriTRUST Essentials & Residential **2018.02.05 Update (see page 2)

– Critical Vulnerability Assessment January 2018[1]:

In terms of computer security issues, 2018 has already created quite a stir, and Intel—the world's foremost CPU chip manufacturer—is at the heart of much of it. This vulnerability assessment is designed to provide you with the information you need to know, without having to spend hours researching and deciphering the technical jargon.

This information bulletin is provided as a service to all our *integriTRUST Essentials & Residential technology partners.* Let's keep the bad actors at bay!

Intel AMT, Meltdown & Spectre Vulnerabilities at a glance:

There are three vulnerabilities that are currently exposing millions of computer users to serious risks of data loss due to unauthorized access:

- Intel® Management Engine Critical Firmware Update (Intel-SA-00086). This affects nearly every computer running Intel chips since 1995, and many systems built using AMD and ARM-based processors. It also affects Servers and selected IOT[2] devices.
- The processor side-channel vulnerabilities known as "***Meltdown***" and "***Spectre***".
- Intel Active Management Technology, Intel Small Business Technology, and Intel Standard Manageability Escalation of Privilege (Intel-SA-00075). This affects many consumer and business machines built on Intel chips using 1st Gen Cores through 7th Gen Cores, and most business machines built or bought in recent years.

Questions and Answers:

- Am I affected by this vulnerability? *Most certainly yes. Several detection tools are linked to this document to facilitate accurate diagnoses.*
- Can my current antivirus protect against this threat? While possible in theory, this is unlikely in practice. Unlike usual malware, Meltdown and Spectre are hard to distinguish from regular benign applications. However, your antivirus may detect malware which uses the attacks by comparing binaries after they become known.
- Can I tell if I've been a victim of Meltdown and Spectre attacks? *Unfortunately, no, not yet. The proof of concept attacks in controlled environments has left no traces in the forms of traditional logs or footprints.*
- Do workarounds and fixes exist? Yes, there are workarounds and fixes in the form of patches and firmware updates for both families of exploits.

[1] Some of these known vulnerabilities have existed since mid 2017. Recently, INTECH has discovered that most of our new partners' computers are still at risk. Alas, many Tech providers have failed to roll out the critical fixes, or even inform their clients of the potential risks.

[2] IOT = Internet of Things and refers to devices with built-in compute power and network connectivity

IMPACT:

Intel-SA-0086, Meltdown & Spectre:

- The potential impact is far-reaching: Workstations and laptops, mobile devices and applications leveraging cloud-based infrastructure running on vulnerable processors can be exposed to unauthorized access and information theft, including passwords and personal information.
- *Meltdown* can enable hackers to gain privileged access to parts of a computer's memory. This affects Intel processors only.
- *Spectre* can allow attackers to steal information from the core of a system. This affects Intel, AMD and ARM processors.

Can it be fixed? And what's the impact?

- Intel has released a detection tool[3] which will determine if your computer is vulnerable.
- Can it be fixed: Yes, depending on the age of your equipment service policies of your hardware vendor—some companies are not releasing firmware patches for systems they consider end-of-life. Also, please note that further patches and updates may be released to buttress the mitigations currently available. ****UPDATE:** The first round of firmware patches was unsuccessful. Intel disclosed that they were causing reboots, crashes and in some instances, data loss. Microsoft released an out-of-cycle patch to undo the Intel patches. Intel also suggested that people not deploy their initial release.
- The patches will be released by hardware vendors to mitigate these vulnerabilities, once Intel's new microcode has been tested.
- Some software vendors are reporting ~15-30% slowdowns can be expected with some computer workloads after patching these vulnerabilities. This should be considered when deciding whether to patch the vulnerability, especially on older machines that may be struggling to keep up with modern workloads. (At INTECH Computer Solutions Inc., we have patched all our machines, and have not noticed any decrease in workload capability, nor the reboots and crashes reported by many).

Intel-SA-00075 (Intel AMT Vulnerability):

- A bug in Intel's Active Management Technology (AMT), Standard Manageability (ISM) and Small Business Technology (SBT) firmware, that can be potentially exploited to remotely control and infect systems with malware.
- This vulnerability affects only selected Intel-based systems.

Can it be fixed? And what's the impact?

** 2018.02.07 Update:

IN THE WILD: A fake patch for the massive Spectre and Meltdown chip flaws is circulating—a disguise for malware called *Smoke Loader*. Whereas hardware and chip vendors are urging users to update their systems, bad actors are using this media buzz to infiltrate and exfiltrate.

"The Meltdown and Spectre bugs have generated a lot of media attention, and users have been urged to update their machines with fixes made available by various vendors.

While some patches have created more issues than they fixed, we came across a particular one targeted at German users that actually is malware. In fact, German authorities recently warned about phishing emails trying to take advantage of those infamous bugs."

- https://blog.malwarebytes.com/cybercrime/2018/01/fake-spectre-and-meltdown-patch-pushes-smoke-loader/

Social engineering efforts by cyber criminals often leverage headline-grabbing issues in an attempt to infect users. This is especially true of high-profile vulnerabilities. Fake patches and fixes were rampant after the critical WannaCry ransomware attack, so it was only a matter of time before Spectre and Meltdown were used by criminals too.

February 7, 2018 Update:
Intel has released *production microcode*—a second round of updates to its OEM partners, for specific platforms and expects to expand this release in the coming days. This means another round of firmware updates from hardware vendors is forthcoming.

[3] Detection tool link: https://downloadcenter.intel.com/download/27150 instructions on its user can be found here.

Tallis Newkirk
tallis@intechcs.ca
306.914.0846

- Intel has developed and released a detection tool[4] which will determine if your computer is vulnerable. The usage instructions are found here.
- Can it be fixed: yes, depending on the age of your equipment service policies of your hardware vendor—some companies are not releasing firmware patches for systems they consider end-of-life. Also, please note that further patches and updates may be released to buttress the mitigations currently available.
- Some hardware and software vendors are reporting slowdowns with some computer workloads after patching these vulnerabilities. This should be considered when deciding whether to patch the vulnerability. (At INTECH Computer Solutions Inc., we have patched all our machines).

Remediation:

Please note: the detection of vulnerability is moderately simple, but the steps to remediation are considerably more involved, requiring familiarity with, and use of the *command prompt* with elevated privileges. INTECH rates these procedures at 7 in terms of difficulty for the average user.

1. Download the detection tool(s) (Intel-SA-00086 and Intel-SA-00075) appropriate for your computer (hardware and operating system).
2. Install or run the detection tools—the GUI based version is sufficient to diagnose your computers.
3. For machines that prove susceptible to the vulnerabilities, download patches relevant to your system from your hardware vendors (i.e. if you are using an HP machine, then HP is your hardware vendor).
4. The patch package should contain documentation including installation instructions. Follow the instructions from your hardware vendor and read through them prior to beginning. If you do not understand anything within the installation guides, do not proceed without the guidance of assistance of your trusted IT professional.
5. If you are unclear with any of the steps detailed in your hardware vendor's instructions, seek the advice and assistance of your trusted Technician.

What can INTECH's integriTRUST Essentials & Residential technology partners expect?

If your computer is monitored by INTECH Computer Solutions Inc.'s *integriTRUST Essentials* or *integriTRUST Residential* services, then we've got your back! In addition to this document, you will receive further communication pertaining to your monitored machines and our thoughts concerning the best course of action for your devices. In some cases, we will want to connect remotely to run the diagnostic tools provided by Intel to determine the scope of the vulnerabilities as they pertain to your assets, before providing a best-practise course of action.

The steps to remediation listed above are provided for your information—**if you are an INTECH partner, please let us implement the fixes.** In most cases, INTECH can apply these patches remotely. If you are not an INTECH client, we recommend enlisting the assistance of qualified IT professionals.

Our *integriTRUST Essentials Commercial & Residential technology partners* can book a time for the remote session, or call us at their convenience. *integriTRUST technology partners* should consult their SLAs to determine their coverage eligibility, or call for an estimate.

Please note we will only be deploying the recommended, tested and proven patches to update the hardware for which it is released.

[4] Detection tool found here: https://downloadcenter.intel.com/download/26755/INTEL-SA-00075-Detection-and-Mitigation-Tool.

Tallis Newkirk
tallis@intechcs.ca
306.914.0846

Contact us today for more information, or click here[5] to book your remediation appointment online. Enjoy the peace of mind that comes with integriTRUST Comprehensive Managed IT Services and Solutions, for commercial and residential partners.

Tallis Newkirk | INTECH Computer Solutions Inc.
tallis@intechcs.ca | 306.914.0846 | www.intechcs.ca

[5] To book INTECH for vulnerability remediation, click here:
https://outlook.office365.com/owa/calendar/INTECHComputerSolutionsInc@intechcs.ca/bookings/