CPU Spectre attacks like a Jedi

bebee.com/producer/cpu-spectre-attacks-like-a-jedi

Published on January 4, 2018 and updated on January 12, 2018

Introduction

Security researchers have found serious vulnerabilities in chips made by Intel and other companies that if exploited could leave passwords and other sensitive data exposed.

Some proof-of-concepts are available for Intel, AMD and ARM CPUs. Spectre may also work better in exploiting cloud systems, it can trick a hypervisor into leaking secrets to a guest.

Think of a Star Wars movie where someone wants to steal money, Spectre is like a Jedi mind trick while Meltdown works like a quick pick-pocket, instead.

Every user on the planet may need to update.

Mashable informs us that these flaws impact almost all of us

[...]

To make matters worse, this vulnerability is the definition of widespread. Bloomberg notes that approximately 90 percent of servers and laptops have Intel chips.

[...]

Intel has finally released a statement about the reported vulnerability, and in it claims that this is not just a problem with its own processors.

> Recent reports that these exploits are caused by a 'bug' or a 'flaw' and are unique to Intel products are incorrect," reads the press release. "Based on the analysis to date, many types of computing devices — with many different vendors’ processors and operating systems — are susceptible to these exploits.

And while this is definitely bad, Intel did hit us with a little bit of good news — namely, that the fix shouldn't slow down computers too much.

> Contrary to some reports, any performance impacts are workload-dependent, and, for the average computer user, should not be significant and will be mitigated over time.

[...]

Summarizing

Because the hardware itself could not fixed some mitigation patches should applied at operative system level for those devices for which is possible. Mitigations patches will make these flaws more difficult to exploit.

Intel acknowledges chip-level security vulnerability in processors

[...]

According to CNET

> Several researchers, including a member of Google's Project Zero team, found that a design technique used in chips from Intel, Arm and others could allow hackers to access data from the memory on your device. The problem impacts processors going back more than two decades and could let hackers access passwords, encryption keys or sensitive information open in applications.

The discovery comes shortly after the chipmaker said it was working on a patch.

[...]

Massive Intel vulnerabilities just landed

[...]

Dubbed Meltdown, the flaw allowed a hacker to read information from applications' memory at the kernel level, a space deep down in the operating system that's core to the functioning of everything on a computer. Passwords, photos, documents and other sensitive data could all be read by an attacker exploiting Meltdown, the researchers warned on a website and in a whitepaper Wednesday. They noted that "virtually every user of a personal computer" in the world was affected either by Meltdown or a related issue they named Spectre, and that the entire memory contents of a vulnerable PC could be surveilled.

If a computer is run by any Intel processor from 1995 onwards, bar Itanium and Atom chips manufactured before 2013, it's likely vulnerable, the researchers warned. And, crucially, cloud environments are also affected, as the flaw could be abused by an attacker to read memory of a virtual machine without any permissions or privileges.

[...]

Reading privileged memory with a side-channel

Project Zero, Wednesday, January 3, 2018

[...]

We have discovered that CPU data cache timing can be abused to efficiently leak information out of mis-speculated execution, leading to (at worst) arbitrary virtual memory read vulnerabilities across local security boundaries in various contexts.

Variants of this issue are known to affect many modern processors, including certain processors by Intel, AMD and ARM. For a few Intel and AMD CPU models, we have exploits that work against real software. We reported this issue to Intel, AMD and ARM on 2017-06-01.

[...]

CPU Spectre attack works like a Jedi mind trick

Spectre may also work better in exploiting cloud systems, according to Gruss. He noted that Spectre can trick a hypervisor – the software that manages virtual machines in a cloud – into leaking secrets to a guest. And, whilst he said it was not as easy to execute as Meltdown, he believes a hack can run in JavaScript. "This means that you would only have to navigate to an attacker-controlled website," he added.

[...]

For a less technical description, Gruss explained:

> Think of a Star Wars movie where someone wants to steal money. Spectre is like a Jedi mind trick: you make someone else give you their money, this happens so quick that they don’t realize what they’re doing.
> Meltdown just grabs the money very quickly like a pickpocket. The Jedi mind trick is of course more difficult to do, but also harder to mitigate.

Google’s products list mitigations

This link above lists affected Google products and their current status of mitigation against CPU speculative execution attack methods. Mitigation Status refers to our mitigation for currently known vectors for exploiting the flaw described in CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

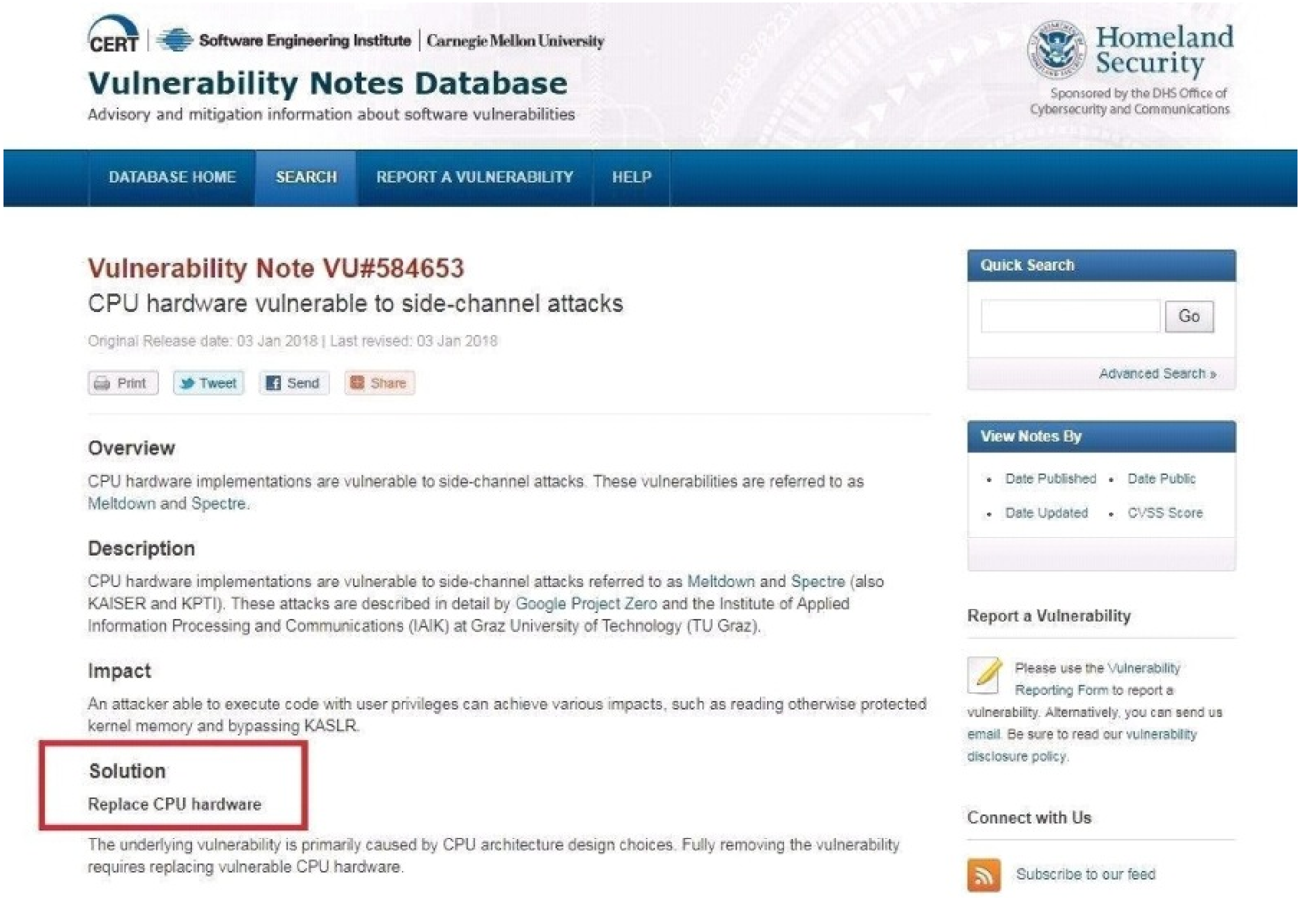
The issue has been mitigated in many Google products (or wasn’t an issue in the first place). In some instances users and customers may need to take additional steps to ensure they’re using a protected version of a product, as detailed below.

This list and a product’s status may change as new developments warrant.

Solution suggested by CERT

Replace the CPU hardware. The underlying vulnerability is primarily caused by CPU implementation optimization choices. Fully removing the vulnerability requires replacing vulnerable CPU hardware.

Apply updates. Operating system updates mitigate the underlying hardware vulnerability



Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

Sponsored by the DHS Office of Cybersecurity and Communications

Vulnerability Note VU#584653

CPU hardware vulnerable to side-channel attacks

Original Release date: 03 Jan 2018 | Last revised: 03 Jan 2018

Overview

CPU hardware implementations are vulnerable to side-channel attacks. These vulnerabilities are referred to as Meltdown and Spectre.

Description

CPU hardware implementations are vulnerable to side-channel attacks referred to as Meltdown and Spectre (also KAISER and KPTI). These attacks are described in detail by Google Project Zero and the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology (TU Graz).

Impact

An attacker able to execute code with user privileges can achieve various impacts, such as reading otherwise protected kernel memory and bypassing KASLR.

Solution

Replace CPU hardware

The underlying vulnerability is primarily caused by CPU architecture design choices. Fully removing the vulnerability requires replacing vulnerable CPU hardware.

Report a Vulnerability

Please use the Vulnerability Reporting Form to report a vulnerability. Alternatively, you can send us email. Be sure to read our vulnerability disclosure policy.

Connect with Us

Updated to add

CERT has downgraded on January 5th, its advice from "replace CPU" to "apply updates."

Spectre and Meltdown are not alone

In fact, a new security flaw detected in Intel BIOS on January 12th, 2018. It has nothing to do with the Spectre and Meltdown vulnerabilities, but also has a huge destructive potential and could be exploited by remote allowing attackers to take complete control over a user's device in a matter of seconds.

Insecure defaults in Intel's Active Management Technology (AMT) allow an intruder to completely bypass user and BIOS passwords and TPM and Bitlocker PINs to backdoor almost any corporate laptop in a matter of seconds.

Harry Sintonen, the F-Secure consultant who discovered the flaw also said

> *The* issue potentially affects millions of laptops globally. It's of an almost shocking simplicity, but its destructive potential is unbelievable.

Loss of confidentiality

F-Secure said once an attacker had the chance to reconfigure AMT the device could be fully controlled remotely by connecting to the same wireless or wired network as the user.

Sintonen warned that

> *No other security measures like full-disk encryption, local firewall, anti-malware software or VPN technology are able to prevent exploitation of this issue.*

Breaking into BIOS allows hackers to access by remote any information and executable instructions even before a piece of installed software.