Foreshadow (security vulnerability)

A logo created for the vulnerability, featuring a lock with a shadow

Foreshadow is a vulnerability that affects modern microprocessors that was first discovered by two independent teams of researchers in January 2018, but was first disclosed to the public on 14 August 2018.[1][2][3][4][5][6][7][8][9][10][11][12] The vulnerability is a speculative execution attack on Intel processors that may result in the loss of sensitive information stored in personal computers or third party clouds.[1] There are two versions: the first version (original/Foreshadow) (CVE-2018-3615 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3615)) targets data from SGX enclaves; and the second version (next-generation/Foreshadow-NG) (CVE-2018-3620 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3620) and CVE-2018-3646 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3646)) targets Virtual Machines (VMs), hypervisors (VMM), operating system (OS) kernel memory, and System Management Mode (SMM) memory.[1] Intel considers the entire class of speculative execution side channel vulnerabilities as "L1 Terminal Fault" (L1TF).[1] A listing of affected Intel hardware has been posted.[9][10]

Foreshadow is similar to the Meltdown and Spectre security vulnerabilities discovered earlier to affect Intel and AMD chips.[6] However, AMD products, according to AMD, are not affected by the Foreshadow security flaws.[6] Nonetheless, one of the variants of Foreshadow goes beyond Intel chips with SGX technology, and affects "all [Intel?] Core processors built over the last seven years".[2]

Foreshadow, according to computer experts, is very difficult to exploit, and there has been no evidence to date (15 August 2018) of any serious hacking involving the Foreshadow vulnerabilities.[6] Applying software patches may help alleviate the problem(s) although the balance between security and performance may be a worthy consideration.[5] Companies performing cloud computing may see a significant decrease in their overall computing power; individuals, however, may not likely see any performance impact, according to researchers.[8] The real fix, according to Intel, is by replacing today's processors.[5] Intel further states, "These changes begin with our next-generation Intel Xeon Scalable processors (code-named Cascade Lake), as well as new client processors expected to launch later this year [2018]."[5]

On 16 August 2018, researchers will present details of the Foreshadow security vulnerabilities in a seminar entitled "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution" at a Usenix Security conference.[7]

Contents

History

Two groups of researchers discovered the security vulnerabilities independently: a Belgian team (including Jo Van Bulck, Frank Piessens, Raoul Strackx) from imec-DistriNet, KU Leuven reported it to Intel on 3 January 2018; a second team from Technion (Marina Minkin, Mark Silberstein), University of Adelaide (Yuval Yarom) and University of Michigan (Ofir Weisse, Daniel Genkin, Baris Kasikci, Thomas F. Wenisch) reported it on 23 January 2018.[1][3] The vulnerabilities were first disclosed to the public on 14 August 2018.[1][3]

Detailed explanation

The Foreshadow vulnerability is a speculative execution attack on Intel processors that may result in the loss of sensitive information stored in personal computers or third party clouds.[1] There are two versions: the first version (original/Foreshadow) (CVE-2018-3615 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3615) [attacks SGX]) targets data from SGX enclaves; and the second version (next-generation/Foreshadow-NG) (CVE-2018-3620 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3620) [attacks the OS Kernel and SMM mode] and CVE-2018-3646 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3646) [attacks virtual machines]) targets Virtual Machines (VMs), hypervisors (VMM), operating system (OS) kernel memory, and System Management Mode (SMM) memory.[1] Intel considers the entire class of speculative execution side channel vulnerabilities as "L1 Terminal Fault" (L1TF).[1]

For Foreshadow, the sensitive data of interest is the encrypted data in an SGX enclave. Usually, an attempt to read enclave memory from outside the enclave is made, speculative execution is permitted to modify the cache based on the data that was read, and then the processor is allowed to block the speculation when it detects that the protected-enclave memory is involved and reading is not permitted. However, "... if the sensitive data is in level 1 cache, speculative execution can use it *before* the processor determines that there's no permission to use it."[3] The Foreshadow attacks are stealthy, and leave few traces of the attack event afterwards in a computer's logs.[4]

Impact

Foreshadow is similar to the Meltdown and Spectre security vulnerabilities discovered earlier to affect Intel and AMD chips.[6] However, AMD products, according to AMD, are not affected by the Foreshadow security flaws.[6] Nonetheless, one of the variants of Foreshadow goes beyond Intel chips with SGX technology, and affects "all [Intel?] Core processors built over the last seven years".[2]

Intel notes that the Foreshadow flaws could produce the following:[5]

- Malicious applications, which may be able to infer data in the operating system memory, or data from other applications.
- A malicious guest virtual machine (VM) may infer data in the VM's memory, or data in the memory of other guest VMs.
- Malicious software running outside of SMM may infer data in SMM memory.
- Malicious software running outside of an Intel SGX enclave or within an enclave may infer data from within another Intel SGX enclave.

According to one of the discoverers of the computer flaws: "... the SGX security hole can lead to a "Complete collapse of the SGX ecosystem."[5]

A listing of affected Intel hardware has been posted, and are described below.[9][10]

- Intel Core i3/i5/i7/M processor (45nm and 32nm)
- 2nd/3rd/4th/5th/6th/7th/8th generation Intel Core processors
- Intel Core X-series processor family for Intel X99 and X299 platforms
- Intel Xeon processor 3400/3600/5500/5600/6500/7500 series
- Intel Xeon Processor E3 v1/v2/v3/v4/v5/v6 family
- Intel Xeon Processor E5 v1/v2/v3/v4 family
- Intel Xeon Processor E7 v1/v2/v3/v4 family
- Intel Xeon Processor Scalable family
- Intel Xeon Processor D (1500, 2100)

Foreshadow, according to computer experts, is very difficult to exploit, and there has been no evidence to date (15 August 2018) of any serious hacking involving the Foreshadow vulnerabilities.[6]

Mitigation

Applying software patches may help alleviate the problem(s) although the balance between security and performance may be a worthy consideration.[5] Companies performing cloud computing may see a significant decrease in their overall computing power; individuals, however, may not likely see any performance impact, according to researchers.[8]

The real fix, according to Intel, is by replacing today's processors.[5] Intel further states, "These changes begin with our next-generation Intel Xeon Scalable processors (code-named Cascade Lake), as well as new client processors expected to launch later this year [2018]."[5]

References

1. Staff (14 August 2018). "Foreshadow - Breaking the Virtual Memory Abstraction with Transient Out-of-Order Execution" (https://foreshadowattack.eu/). *ForeShadowAttack.eu*. Retrieved 14 August 2018.
2. Kan, Michael (14 August 2018). "New 'Foreshadow' Flaw Exploits Intel Chips To Steal Protected Data - The new vulnerability builds on research related to the Meltdown and Spectre flaws. Foreshadow can be exploited to read data from Intel's SGX technology, while a separate variant can break the security protections in data centers that run virtual machines" (https://www.pcmag.com/news/363105/new-foreshadow-flaw-exploits-intel-chips-to-steal-protecte). *PC Magazine*. Retrieved 14 August 2018.
3. Bright, Peter (14 August 2018). "Intel's SGX blown wide open by, you guessed it, a speculative execution attack - Speculative execution attacks truly are the gift that keeps on giving" (https://arstechnica.com/gadgets/2018/08/intels-sgx-blown-wide-open-by-you-guessed-it-a-speculative-execution-attack/). *Ars Technica*. Retrieved 14 August 2018.
4. Newman, Lily Hay (14 August 2018). "Spectre-like Flaw Undermines intel Processors' Most Secure Element" (https://www.wired.com/story/foreshadow-intel-secure-enclave-vulnerability/). *Wired*. Retrieved 15 August 2018.
5. Vaughan-Nichols, Steven J. (14 August 2018). "Beyond Spectre: Foreshadow, a new Intel security problem - Researchers have broken Intel's Software Guard Extensions, System Management Mode, and x86-based virtual machines" (https://www.zdnet.com/article/beyond-spectre-foreshadow-a-new-intel-security-problem/). *ZDNet*. Retrieved 15 August 2018.
6. Giles, Martin (14 August 2018). "Intel's 'Foreshadow' flaws are the latest sign of the chipocalypse" (https://www.technologyreview.com/the-download/611879/intels-foreshadow-flaws-are-the-latest-sign-of-the-chipocalypse/). *MIT Technology Review*. Retrieved 14 August 2018.
7. Chirgwin, Richard (15 August 2018). "Foreshadow and Intel SGX software attestation: 'The whole trust model collapses' - El Reg talks to Dr Yuval Yarom about Intel's memory leaking catastrophe" (https://www.theregister.co.uk/2018/08/15/foreshadow_sgx_software_attestations_collateral_damage/). *The Register*. Retrieved 15 August 2018.
8. Lee, Dave (15 August 2018). "'Foreshadow' attack affects Intel chips" (https://www.bbc.com/news/technology-45191697). *BBC News*. Retrieved 15 August 2018.
9. Staff (14 August 2018). "Q3 2018 Speculative Execution Side Channel Update (Intel-SA-00161)" (https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html). *Intel*. Retrieved 1 August 2018.
10. Armasu, Lucian (15 August 2018). "Intel Chips' List of Security Flaws Grows" (https://www.tomshardware.com/news/intel-chips-foreshadow-security-flaws,37608.html). *Tom's Hardware*. Retrieved 15 August 2018.
11. Kerner, Sean Michael (15 August 2018). "Intel SGX at Risk From Foreshadow Speculative Execution Attack - Another set of side-channel, speculative execution vulnerabilities have been publicly reported by security researchers; this time the vulnerabilities take specific aim at SGX secure enclave and hypervisor isolation boundaries" (http://www.eweek.com/security/intel-sgx-at-risk-from-foreshadow-speculative-execution-attack). *eWeek*. Retrieved 15 August 2018.
12. Kennedy, John (15 August 2018). "A Foreshadow of security: What you need to know about new Intel chip flaws" (https://www.siliconrepublic.com/enterprise/foreshadow-intel-vulnerabilities-chips-sgx). *Silicon Republic.com*. Retrieved 15 August 2018.

External links

- Official WebSite (https://ForeShadowAttack.eu)
- Meltdown/Spectre Checker (https://www.grc.com/inspectre.htm) Gibson Research Corporation
- Foreshadow – overview (video; 03:09) (https://www.youtube.com/watch?v=ynB1inl4G3c) on YouTube
- Foreshadow – technical (video; 00:40) (https://www.youtube.com/watch?v=8ZF6kX6z7pM) on YouTube