OTHER CPU SIDE-CHANNEL VULNERABILITIES

PUBLISHED: DECEMBER 14, 2018 | LAST UPDATE: JUNE 20, 2022

Summary

Over the course of 2018 -2022 industry researchers disclosed a variety of side-channel vulnerabilities for contemporary processor technologies in addition to the more notable Meltdown and Spectre exposures. These additional variants of side-channel vulnerabilities share the same exposures as Meltdown and Spectre for A10 products and are separately addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2018-0495	CVSS 3.0	5.1 Med	ROHNP - Key Extraction Side Channel in Multiple Crypto Libraries
2	CVE-2018-3615	CVSS 3.0	6.3 Med	L1 Terminal Fault-SGX (aka Foreshadow)
3	CVE-2018-3620	CVSS 3.0	5.6 Med	L1 Terminal Fault-OS/SMM
4	CVE-2018-3646	CVSS 3.0	5.6 Med	L1 Terminal Fault-VMM
5	CVE-2018-3665	CVSS 3.0	5.6 Med	Kernel: FPU state information leakage via lazy FPU restore
6	CVE-2018-5407	CVSS 3.0	4.8 Med	Intel processor side-channel vulnerability on SMT/Hyper-Threading architectures (PortSmash)
7	A10-2019-0001	A10	Low	SPOILER: Speculative Load Hazards Boost Rowhammer and Cache Attacks [(i)]
8	CVE-2018-12126	CVSS 3.0	6.5 Med	x86: Microarchitectural Store Buffer Data Sampling - MSBDS (Fallout)
9	CVE-2018-12127	CVSS 3.0	6.5 Med	x86: Microarchitectural Load Port Data Sampling - Information Leak - MLPDS
10	CVE-2018-12130	CVSS 3.0	6.2 Med	x86: Microarchitectural Fill Buffer Data Sampling - MFBDS (Fallout, RIDL)
11	CVE-2019-11091	CVSS 3.0	3.8 Low	x86: Microarchitectural Data Sampling Uncacheable Memory - MDSUM
12	CVE-2019-11184	CVSS 3.0	4.8 Med	hardware: Side-channel cache attack against DDIO with RDMA (NetCat)
13	CVE-2020-0548	CVSS 3.0	2.3 Low	hw: Vector Register Data Sampling (CacheOut)
14	CVE-2020-0549	CVSS 3.0	6.5 Med	hw: L1D Cache Eviction Sampling (CacheOut)
15	CVE-2021-33149	CVSS 3.1	2.5 Low	hw: cpu: CVE-2021-33149 – Intel(R) Processor Speculative Cross Store Bypass Advisory

[(i)] Can only affect vThunder deployments on Intel Core CPUs.

These vulnerabilities take advantage of weaknesses in the implementation of computer systems using most (if not all) modern processors and Operating Systems (OSs), including those supported by A10 products. They could allow an unprivileged attacker, in specific circumstances, to read privileged memory belonging to other processes or memory allocated to the Operating System (OS) kernel. To successfully exploit these weaknesses and gain access to restricted memory, an attack requires the execution of crafted, custom code on the target device or system.

ACOS products that support the External Health Monitor feature are potentially exposed to misuse of the feature by malicious, Read-Write privileged administrators. Accordingly, A10 recommends limiting access to such critical infrastructure networking equipment to only trusted administrators from trusted administrative networks and hosts as a defense against

active exploit of these vulnerabilities and to ensure that only code fully-trusted by the customer is deployed to these products.

A10 products and release families that support this ACOS feature and warrant these administrative considerations include:

• Thunder and vThunder	ADC, CGN, SSLi, CFW	ACOS (4.1.4, 4.1.2, 4.1.1, 4.1.0)
• Thunder, vThunder, and AX	ADC	ACOS (2.7.2, 2.7.1-GR1, 2.6.1-GR1)
• Thunder and AX	CGN	ACOS (2.8.2)

A10 aGalaxy and other ACOS products do not support this feature and are accordingly unaffected by these vulnerabilities. These products include:

• Thunder	TPS	ACOS (3.0, 3.1, 3.2, 5.0.x-TPS)
• aGalaxy	TPS Centralized Mgmt	aGalaxy (3.2.x, 5.0.x)
• aGalaxy 5000	TPS Centralized Mgmt	aGalaxy (3.2.x, 5.0.x)
• aGalaxy	ADC Centralized Mgmt	aGalaxy (3.0)

For all virtualized A10 products, including ACOS vThunder, A10 recommends that customers ensure that their Host-OSs (hypervisors) are updated as necessary to address these vulnerabilities and that their underlying platforms have corresponding, appropriate firmware updates.

In addition, for A10 Lightning ADC and Harmony Controller virtualized products, root-level access to the Local OS shell and Container Management System (CMS) software is available to product administrators. A10 recommends that only trusted administrators likewise be allowed access to these root-level, privileged services to ensure that malicious code which could exploit these vulnerabilities does not enter or become established in virtual instances of these products.

For A10 Harmony Controller Appliance and Hybrid Virtual Appliance products, root-level access to the Host OS shell is also available to product administrators. A10 additionally recommends that only trusted administrators likewise be allowed access to this service to ensure that potentially malicious code from untrusted parties does not become instantiated in these appliances.

To improve the ability of customers to manage ACOS devices, in light of these issues and others like them in the future, A10 will harden and enhance ACOS configuration and management capabilities for this feature as described in the Affected Releases section below. The table below indicates releases of ACOS exposed to this vulnerability and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

A10 will investigate future side-channel vulnerabilities for potential impacts and will update this advisory as additional information becomes available. As this investigation proceeds, A10 PSIRT looks forward to feedback and questions on these issues. Customers and partners are welcome to contact the A10 Technical Assistance Center (TAC) or their A10 Sales Representatives. Others are invited to contact A10 PSIRT via email.

Affected Releases

The table below indicates releases of A10 products potentially exposed to misuse of this ACOS configuration management feature by malicious, Read-Write privileged administrators and releases that will harden and enhance ACOS configuration management for this feature.

Customers using potentially exposed releases can update ACOS to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no release update is currently available or anticipated.

Releases Affected			Releases Resolved or Unaffected
4.1.4	–	4.1.4-P2	4.1.4-P3, 4.1.4-GR1, 5.x.x
4.1.2	–	4.1.2-P4	4.1.2-P5, 4.1.4-GR1, 5.x.x
4.1.1	–	4.1.1-P9	4.1.1-P10, 4.1.4-GR1, 5.x.x
4.1.100	–	4.1.100-P5-SP1	4.1.100-P6 [(a)]
4.1.0	–	4.1.0-P11	4.1.0-P12, 4.1.4-GR1, 5.x.x
4.0.0	–	4.0.3-P4	4.1.0-P12, 4.1.1-P10, 4.1.4-P3, 4.1.4-GR1, 5.x.x
2.8.2	–	2.8.2-P10	4.1.2-P5, 4.1.4-P3, 4.1.4-GR1, 5.x.x
2.7.2	–	2.7.2-P13	4.1.0-P12, 4.1.1-P10, 4.1.4-P3, 4.1.4-GR1, 5.x.x
2.7.1-GR1	–	2.7.1-GR1-Px	4.1.0-P12, 4.1.1-P10, 4.1.4-P3, 4.1.4-GR1, 5.x.x
2.6.1-GR1	–	2.6.1-GR1-P16	4.1.0-P12, 4.1.1-P10, 4.1.4-P3, 4.1.4-GR1, 5.x.x

[(a)] Summarily disabled the External Health Monitor feature.

Workarounds and Mitigations

General, recommended practices for the administration of A10 products are described in the Summary section above regarding these potential exposures. Other specific workarounds or mitigations are described below.

Restricting Extended Health Monitor Access

For A10 products with an ACOS 4.1.x release, before 4.1.4-GR1, and which are using local database authentication for administration, a workaround is available to restrict administrators' use of the External Health Monitor feature.

For such configurations, include the following Role-Based Access (RBA) configuration constraint for all ACOS administrators except those sufficiently trusted to ensure that the ACOS system is not exposed to potentially malicious code, either by their malicious use or by compromise of their administrative systems.

1. Enable RBA (if not already enabled)

```
ACOS(config)# rba enable
```

2. Apply the constraint for all system-wide (shared partition) administrative users. The CLI example below uses `adminuser1` for the username of the account.

```
ACOS(config)# rba user adminuser1
ACOS(config-user:adminuser1)# partition shared
ACOS(config-user:adminuser1-partition:sh...)#import.health-external no-access
```

3. Apply the constraint for all Application Delivery Partition (ADP) administrative users. The CLI example below uses `adminuser5` and `partition-5` for the username and partition of the account; respectively.

```
ACOS(config)# rba user adminuser5
ACOS(config-user:adminuser5)# partition partition-5
ACOS(config-user:adminuser5-partition:pa...)#import.health-external no-access
```

4. If the External Health Monitor feature is not used in the A10 product's deployment scope, stop here.

5. If the administration policy of the A10 product is to only trust the ACOS default (root) administrator account (username `admin`) in this regard, stop here.

6. Otherwise, remove the constraint for the select administrative user(s) sufficiently trusted for this administrative capability. The CLI example below uses `adminuser3` for the username of the account.

```
ACOS(config)# rba user adminuser3
ACOS(config-user:adminuser3)# partition shared
ACOS(config-user:adminuser3-partition:sh...)#import.health-external write
```

For partition constrained administrative users:

```
ACOS(config)# rba user adminuser5
ACOS(config-user:adminuser5)# partition partition-5
ACOS(config-user:adminuser5-partition:pa...)#import.health-external write
```

Reviewing Extended Health Monitor Configuration

External health monitor scripts should be reviewed and audited to ensure their integrity and intended use in the ACOS system. Instantiated scripts can be listed by the **`show health external`** ACOS CLI command and inspected individually using the **`show health external file.ext`** ACOS CLI command, where **`file.ext`** is the of the indicated script files listed.

Monitoring Extended Health Monitor Activity

External health monitor activity can be monitored via the ACOS Audit Log. This log can be configured to log events to an external server through the **`logging auditlog host`** CLI command. Import operations can be detected on the logging server by filtering for the following strings and reporting match events for administrative review.

- For ACOS 4.x Systems: import health-external
- For ACOS 2.x Systems: health external import

Software Updates

Software updates that address these vulnerabilities are or will be published at the following URL:

https://support.a10networks.com/

Vulnerability Details

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2018-0495	Libgcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signatures that can be mitigated through the use of blinding during the signing process in the _gcry_ecc_ecdsa_sign function in cipher/ecc-ecdsa.c, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.
CVE-2018-3615	Systems with microprocessors utilizing speculative execution and Intel software guard extensions (Intel SGX) may allow unauthorized disclosure of information residing in the L1 data cache from an enclave to an attacker with local user access via a side-channel analysis.
CVE-2018-3620	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis.

CVE-2018-3646	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis
CVE-2018-3665	System software utilizing Lazy FP state restore technique on systems using Intel Core-based microprocessors may potentially allow a local process to infer data from another process through a speculative execution side channel.
CVE-2018-5407	A flaw was found in the Intel processor execution engine sharing on SMT (e.g. Hyper-Threading) architectures. An attacker running a malicious process on the same core of the processor as the victim process, can extract certain secret information. The reporter is able to steal an OpenSSL (<= 1.1.0h) P-384 private key from a TLS server using this new side-channel vector. It is a local attack in the sense that the malicious process must be running on the same physical core as the victim (an openSSL-powered TLS server in this case). But in general any application which branches on a secret value may be affected.
A10-2019-0001	In this work, we are the first to show that the dependency resolution logic that serves the speculative load can be exploited to gain information about the physical page mappings. We propose the SPOILER attack which exploits this leakage to speed up this reverse engineering by a factor of 256. Then, we show how this can improve the Prime+Probe attack by a 4096 factor speed up of the eviction set search, even from sandboxed environments like JavaScript. Finally, we improve the Rowhammer attack by showing how SPOILER helps to conduct DRAM row conflicts deterministically with up to 100% chance, and by demonstrating a double-sided Rowhammer attack with normal user's privilege. The later is due to the possibility of detecting contiguous memory pages using the SPOILER leakage. The leakage can be exploited by a limited set of instructions, which is visible in all Intel generations starting from the 1st generation of Intel Core processors, independent of the OS and also works from within virtual machines and sandboxed environments.
CVE-2018-12126	A flaw was found in many Intel microprocessor designs related to a possible information leak of the processor store buffer structure which contains recent stores (writes) to memory. Modern Intel microprocessors implement hardware-level micro-optimizations to improve the performance of writing data back to CPU caches. The write operation is split into STA (STore Address) and STD (STore Data) sub-operations. These sub-operations allow the processor to hand-off address generation logic into these sub-operations for optimized writes. Both of these sub-operations write to a shared distributed processor structure called the 'processor store buffer'. The processor store buffer is conceptually a table of address, value, and 'is valid' entries. As the sub-operations can execute independently of each other, they can each update the address, and/or value columns of the table independently. This means that at different points in time the address or value may be invalid. The processor may speculatively forward entries from the store buffer. The split design used allows for such forwarding to speculatively use stale values, such as the wrong address, returning data from a previous unrelated store. Since this only occurs for loads that will be reissued following the fault/assist resolution, the program is not architecturally impacted, but store buffer state can be leaked to malicious code carefully crafted to retrieve this data via side-channel analysis. The processor store buffer entries are equally divided between the number of active Hyper-Threads. Conditions such as power-state change can reallocate the processor store buffer entries in a half-updated state to another thread without ensuring that the entries have been cleared. This issue is referred to by the researchers and the industry as Fallout.

CVE-2018-12127	Microprocessors use 'load ports' to perform load operations from memory or IO. During a load operation, the load port receives data from the memory or IO subsystem and then provides the data to the CPU registers and operations in the CPU's pipelines. In some implementations, the writeback data bus within each load port can retain data values from older load operations until newer load operations overwrite that data MLPDS can reveal stale load port data to malicious actors when: * A faulting/assisting SSE/AVX/AVX-512 loads that are more than 64 bits in size * A faulting/assisting load which spans a 64-byte boundary. In the above cases, the load operation speculatively provides stale data values from the internal data structures to dependent operations. Speculatively forwarding this data does not end up modifying program execution, but this can be used as a widget to speculatively infer the contents of a victim process's data value through timing access to the load port.
CVE-2018-12130	This issue has the most risk associated, which Red Hat has rated as Important. A flaw was found by researchers in the implementation of fill buffers used by Intel microprocessors. A fill buffer holds data that has missed in the processor L1 data cache, as a result of an attempt to use a value that is not present. When a Level 1 data cache miss occurs within an Intel core, the fill buffer design allows the processor to continue with other operations while the value to be accessed is loaded from higher levels of cache. The design also allows the result to be forwarded to the Execution Unit, acquiring the load directly without being written into the Level 1 data cache. A load operation is not decoupled in the same way that a store is, but it does involve an Address Generation Unit (AGU) operation. If the AGU generates a fault (#PF, etc.) or an assist (A/D bits) then the classical Intel design would block the load and later reissue it. In contemporary designs, it instead allows subsequent speculation operations to temporarily see a forwarded data value from the fill buffer slot prior to the load actually taking place. Thus it is possible to read data that was recently accessed by another thread if the fill buffer entry is not overwritten. This issue is referred to by researchers and the industry as RIDL or ZombieLoad.
CVE-2019-11091	A flaw was found in the implementation of the "fill buffer," a mechanism used by modern CPUs when a cache-miss is made on L1 CPU cache. If an attacker can generate a load operation that would create a page fault, the execution will continue speculatively with incorrect data from the fill buffer, while the data is fetched from higher-level caches. This response time can be measured to infer data in the fill buffer.
CVE-2019-11184	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access.
CVE-2020-0548	Cleanup errors in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-0549	Cleanup errors in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2021-33149	Observable behavioral discrepancy in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.

Related Links

Ref #	General Link
[1]	NIST NVD, CVE-2018-0495
[2]	NIST NVD, CVE-2018-3615
[3]	NIST NVD, CVE-2018-3620
[4]	NIST NVD, CVE-2018-3646
[5]	NIST NVD, CVE-2018-3665
[6]	NIST NVD, CVE-2018-5407
[7]	White Paper - SPOILER: Speculative Load Hazards Boost Rowhammer and Cache Attacks
[8]	NIST NVD, CVE-2018-12126
[9]	NIST NVD, CVE-2018-12127
[10]	NIST NVD, CVE-2018-12130
[11]	NIST NVD, CVE-2019-11091
[8 - 11]	MDS - Microarchitectural Data Sampling - CVE-2018-12130, CVE-2018-12126, CVE-2018-12127, and CVE-2019-11091
[12]	NIST NVD, CVE-2019-11184
[13]	NIST NVD, CVE-2020-0548
[14]	NIST NVD, CVE-2020-0549
[15]	NIST NVD, CVE-2021-33149

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2018-12-14	Initial Publication
2.0	2019-03-26	Added SPOILER side-channel vulnerability for vThunders deployed on Intel Core CPUs
3.0	2019-05-16	Added ZombieLoad, Fallout, and other side-channel vulnerabilities (CVE-2018-12126/12127/12130 and CVE-2019-11091)
4.0	2019-07-22	Updated legacy ACOS 2.7.2 & 2.8.2 releases to be remediated only by updates to resolved ACOS 4.1.x release families.
5.0	2019-10-11	Added 4.1.100 release family. Added NetCat side-channel vulnerability (CVE-2019-11184).
6.0	2020-02-18	Added CVE-2020-0548/0549
7.0	2022-06-20	Added CVE-2021-33149. Updated resolved/unaffected releases for contemporary release families. Misc other continuity corrections.