Security Advisory

SPECTRE/MELTDOWN VULNERABILITIES

PUBLISHED: JANUARY 5, 2018 | LAST UPDATE: OCTOBER 11, 2019

SUMMARY

On January 3, 2018, researchers disclosed security vulnerabilities known commonly in the industry as Spectre [4] and Meltdown [5]. On May 22, 2018, two variants of the Spectre vulnerability were disclosed [6] in the industry. Subsequently, other variants have been disclosed. Collectively, these vulnerabilities have been assigned the following CVEs:

Item		**Score**		
#	**Vulnerability ID**	**Source**	**Score**	**Summary**
1	CVE-2017-5715	CVSS 3.0	5.6 Med	Speculative execution branch target injection (Spectre) [1]
2	CVE-2017-5753	CVSS 3.0	5.6 Med	Speculative execution bounds-check bypass (Spectre) [2]
3	CVE-2017-5754	CVSS 3.0	5.6 Med	Speculative execution permission faults handling (Meltdown) [3]
4	CVE-2018-3639	CVSS 3.0	5.6 Med	Speculative store bypass (Spectre Variant 4 or SpectreNG) [7]
5	CVE-2018-3640	CVSS 3.0	2.8 Low	Speculative register load (Spectre Variant 3a) [8]
6	CVE-2018-3693	CVSS 3.0	5.6 Med	Speculative bounds check bypass store (Spectre 1.1) [9]
7	CVE-2019-1125	CVSS 3.0	5.6 Med	Spectre SWAPGS gadget vulnerability (Spectre 1 - swapgs) [10]

These vulnerabilities take advantage of implementations for the speculative execution of instructions on 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)
• aGalaxy	TPS Centralized Mgmt	aGalaxy (3.2)
• aGalaxy 5000	TPS Centralized Mgmt	aGalaxy (3.2)
• 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.

A10 continues to investigate the Spectre and Meltdown vulnerabilities for further 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
4.1.2	–	4.1.2-P4	4.1.2-P5
4.1.1	–	4.1.1-P9	4.1.1-P10
4.1.100	–	4.1.100-P5-SP1	4.1.100-P6 [a]
4.1.0	–	4.1.0-P11	4.1.0-P12
4.0.0	–	4.0.3-P4	4.1.0-P12, 4.1.1-P10, 4.1.4-P3
2.8.2	–	2.8.2-P10	4.1.2-P5, 4.1.4-P3
2.7.2	–	2.7.2-P13	4.1.0-P12, 4.1.1-P10, 4.1.4-P3
2.7.1-GR1	–	2.7.1-GR1-Px	4.1.0-P12, 4.1.1-P10, 4.1.4-P3
2.6.1-GR1	–	2.6.1-GR1-P16	4.1.0-P12, 4.1.1-P10, 4.1.4-P3

[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 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:

http://www.a10networks.com/support/axseries/software-downloads

VULNERABILITY DETAILS

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

Vulnerability ID	**Description**
CVE-2017-5715	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2017-5753	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2017-5754	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

CVE-2018-3639 Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.

CVE-2018-3640 Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis, aka Rogue System Register Read (RSRE), Variant 3a.

CVE-2018-3693 Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a speculative buffer overflow and side-channel analysis.

CVE-2019-1125 An attacker can train the branch predictor to speculatively skip the swapgs path for an interrupt or exception. If they initialize the GS register to a user-space value, if the swapgs is speculatively skipped, subsequent GS-related percpu accesses in the speculation window will be done with the attacker-controlled GS value. This could cause privileged memory to be accessed and leaked.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2017-5715
[2]	NIST NVD, CVE-2017-5753
[3]	NIST NVD, CVE-2017-5754
[4]	https://spectreattack.com/
[5]	https://meltdownattack.com/
[6]	US-CERT, Alert (TA18-141A) Side-Channel Vulnerability Variants 3a and 4
[7]	NIST NVD, CVE-2018-3639
[8]	NIST NVD, CVE-2018-3640
[9]	NIST NVD, CVE-2018-3693
[10]	NIST NVD, CVE-2019-1125

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-01-05	Initial Publication
2.0	2018-01-06	Removed template text unrelated to this advisory.
3.0	2018-02-12	Updated Summary, Affected Releases, Workarounds and Mitigations, Vulnerability Details, Related Links
4.0	2018-03-09	Added ACOS 4.1.4 release information
5.0	2018-04-04	Updated ACOS 4.1.0 release information
6.0	2018-06-12	Added new variants – CVE-2018-3639/3640. Updated release information for ACOS 4.1.4, 4.1.2, 4.1.1, 2.7.2. Changed to 'planned' releases for hardening enhancements. Extended workarounds/mitigations. Changed title to remove specific CVEs & make generic for all Meltdown/Spectre family variants.
6.1	2018-06-15	Misc format and retitling changes.
7.0	2018-07-12	Added new variant – Spectre 1.1. Updated release information for 2.7.1-GR1,
8.0	2018-11-09	Updated affected and resolved releases information for ACOS 4.1.1, 2.7.1-GR1, and 2.6.1-GR1 release families.
9.0	2018-11-12	Additional updates to resolved releases information for ACOS 4.1.0, 4.1.1, and 4.1.2 release families.
10.0	2018-12-12	Updated affected and resolved releases information for ACOS 2.7.2 and 2.8.2 release families.
11.0	2018-12-14	Corrected syntax recommendation typos in workarounds and remediations.
12.0	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.
13.0	2019-08-06	Added new SWAPGS variant of Spectre 1, CVE-2019-1125.
14.0	2019-10-11	Added 4.1.100 release family.

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability, non-infringement or fitness for a particular use. Your use of the information in this document or materials linked from this document is at your own risk. A10 Networks, Inc. reserves the right to change or update the information in this document at any time.