12th April, 2018

Security Advisory

Security Vulnerabilities Meltdown and Spectre

Meltdown and Spectre are two related security vulnerabilities affecting products that utilize a wide range of processors by enabling unauthorized information disclosure. Three critical architectural flaws in CPUs have been recently disclosed to date, that allow user processes to read kernel or hypervisor memory through cache side-channel attacks.

Meltdown – exploits a race condition that occurs between memory access and privilege verification during instruction processing. Combined with a cache side-channel attack, it allows a process to sidestep normal access privilege verification, enabling an unauthorized process to read data from any address mapped to the current process memory space.

Spectre – on processors that perform speculative execution, a branch misprediction can result in exposure of private data to attackers. For example, if the pattern of memory access performed by the speculative execution depends on private data, the resulting state of the data cache creates a side channel through which an attacker may be able to extract information about private data using a timing attack.

What is Speculative Execution?

Speculative execution is a technique used by most modern high performance processors to improve performance. Speculative execution carrys out instructions ahead of knowing that they are required, keeping the CPU occupied while it is waiting for a memory load. It is possible for speculative execution to have side effects which are not restored when the CPU state is unwound, which can lead to information disclosure.

To date, 3 variants a related security vulnerability have been reported.

- Spectre (variants 1 and 2)
- Meltdown (variant 3)

1. **CVE-2017-5753: variant 1 - bounds check bypass**
   Local attackers on systems with modern CPUs featuring deep instruction pipe-lining could use attacker controllable speculative execution over code patterns in the Linux kernel to leak content from otherwise unreadable memory in the same address space, allowing retrieval of passwords, cryptographic keys and other confidential information.

2. **CVE-2017-5715: variant 2 - branch target injection**
   Local attackers on systems with modern CPUs featuring branch prediction could use mispredicted branches to speculatively execute code patterns that in turn could be made to leak other non-readable content in the same address space, an attack similar to CVE-2017-5753.

3. **CVE-2017-5754: variant 3 - rogue data cache load**
   Local attackers on systems with modern CPUs featuring deep instruction pipelining could use code patterns in user space to speculative executive code that would read otherwise read protected memory, an attack similar to CVE-2017-5753.

How do the attacks work?

All the attacks result in information leaked from higher privileged or isolated same privileged contexts, typically using an architectural side channel. The premise is that bugs in the CPU speculative execution can alter the micro architectural state, even when the speculated instructions are rolled back. Malicious software can trigger this sequence and then use a side channel to read the information. The side channels typically employed are cache timing side channels. The basic principle behind cache timing side-channels is that the pattern of allocations into the cache, and, in particular, which cache sets have been used for the allocation, can be determined by measuring the time taken to access entries that were previously in the cache, or by measuring the time to access the entries that have been allocated. This then can be used to determine which addresses have been allocated into the cache.

Impact on Kalkitech Products

With the available information to date from various public announcements and published vendor information, we have assessed the products listed below, some of which are vulnerable to Meltdown and Spectre. We are actively monitoring updates from vendors and as additional information or changes become available that changes the information below, we will publish an update to this Security Advisory.

Series	Processor/Soc Vendor	Meltdown	Spectre
SYNC 211	Digi	No	No
SYNC 221	Microchip	No	No
SYNC 241	Microchip	No	No
SYNC 261	Texas Instruments	No	Yes
SYNC 941/943	ST-Microelectronics	No	No
SYNC 1811	ST-Microelectronics	No	No
SYNC 1851	ST-Microelectronics	No	No
SYNC 1911	Microchip	No	No
SYNC 2000	Microchip	No	No
SYNC 2101	Microchip	No	No
SYNC 2111	Microchip	No	No
SYNC 3000	NXP	No	Yes
SYNC 4000	Intel	Yes	Yes
ASE 2000 - BCOM-USB Device	ST Microelectronics	No	No
ASE Bell 202 Modems (Box / Rack)	Microchip	No	No
ASE SPTSRV-4	Microchip	No	No

ASE SPTSRV-8	Microchip	No	No
ASE SPTSRV-16	Microchip	No	No
ASE ARMNET-4	Microchip	No	No
ASE BCOM-TSRV	Microchip	No	No
ASE SAM - 900	Intel [AAEON-PC]	No	No
ASE - Older Versions of SPT	AMD	No	No

What should Customers do if their Kalkitech product is listed as vulnerable?

SYNC 261 and SYNC 3000

Vulnerabilities exposed by Spectre are characterized by the need to download a malicious executable code to the device under attack to run on the device and exploit the vulnerability to gain access to unauthorized memory. The typical scenarios being used to describe these exploits revolve around desktop systems and servers where applications like browsers connect to remote machines and present opportunities to run code downloaded from those remote machines, thereby providing a natural path for malicious code to enter the system.

SYNC261 and SYNC3000 are embedded and highly “closed” devices which provide no options to download and execute external code during regular operation. To exploit the vulnerability presented by Meltdown and Spectre, a malicious user must explicitly gain access to install executable programs and then use that access to install into the device custom software designed to use the vulnerability. If the operating environment of these devices provide for standard physical and network security, the opportunities for this exploit may be greatly diminished or non-existent. Hence from the viewpoint of their embedded nature and the resulting diminished attack surface they present, SYNC261 and SYNC3000 users may not be required to take any actions to protect their devices against these vulnerabilities.

As soon as new Linux kernels are available from processor / operating system vendors that address this fix and can be integrated into these platforms, we will notify our customers.

SYNC 4000

SYNC 4000 devices deploy Kalkitech protocol software solutions on a off-the-shelf server hardware installed with off-the-shelf Linux distribution. Therefore, the SYNC 4000 is vulnerable to the exploits presented by Meltdown and Spectre. Specifically, the vulnerabilities are not created or introduced by Kalkitech’s application software but exist as a result of the processor design and the way that the Operating System uses it. The protective measures to mitigate this vulnerability is currently limited to software fixes in the Operating System. These fixes are expected to be delivered by the Operating System vendors and Kalkitech is monitoring the situation closely to identify the appropriate fix.

12th April, 2018

In General, please follow these guidelines for all products supplied by Kalkitech:

1. Since these security vulnerabilities can be exploited only if external software is installed on our products, that can exploit this vulnerability, Kalkitech recommends not to run any software other than that is supplied by Kalkitech.
2. Kalkitech also recommends our products be always used within your internal firewall and not exposed to the Internet or even business IT systems, if possible.
3. If you are unsure of the authenticity of any of Kalkitech software delivered, please request an SHA key to verify it before you install it.
4. Please keep updating the firmware and kernel from time-to-time and register in our support portal to receive notices. All our customers with an active warranty receive updates from us on new releases to firmware and kernel, when available from Operating System Vendors for the affected processors used in our products.

We will revise this Notice with updates as more information becomes available from Operating System and Processor vendors. General announcements will be available on our website as to affected hardware, while specific actions that affect you will be separately intimated and driven by Kalkitech Security Policy.

Support

For any additional information or specific questions, please contact our support at support@kalkitech.com or support@ase-systems.com. Please also visit our website for any new updates.

References

NIST CVE 2017-5715
https://nvd.nist.gov/vuln/detail/CVE-2017-5715

NIST CVE 2017-5753
https://nvd.nist.gov/vuln/detail/CVE-2017-5753

NIST CVE-2017-5754
https://nvd.nist.gov/vuln/detail/CVE-2017-5754

https://googleprojectzero.blogspot.in/2018/01/reading-privileged-memory-with-side.html

Update from CPU Vendors

AAEON
http://www.aaeon.com/en/ni/security-announcement-intel-side-channel-vulnerability

12th April, 2018

ARM
Comprehensive list of affected ARM CPUs.
https://developer.arm.com/support/security-update

Intel
https://newsroom.intel.com/wp-content/uploads/sites/11/2018/01/Intel-Analysis-of-Speculative-Execution-Side-Channels.pdf

NXP
While from NXP at this time we do not have a public statement on the specific NXP processor in SYNC 3000, they did inform Kalkitech that the processor used in SYNC 3000 is affected by Spectre, but not Meltdown; They are determining the migration strategy and will update us when that is available; For a highly closed embedded system, the mitigation strategy could be “no action required”.

Texas Instruments
https://e2e.ti.com/support/arm/sitara_arm/f/791/t/654938