Sierra Wireless Security Advisory SWI-PSA-2018-001: Spectre/Meltdown Vulnerabilities

Release Date: January 12, 2018, revision 1

Issue Description:

Google Project Zero has released information regarding vulnerabilities in multiple modern CPU architectures that allow side-channel leakage of information through three variants identified as follows:

- Variant 1: bounds check bypass (CVE-2017-5753)
- Variant 2: branch target injection (CVE-2017-5715)
- Variant 3: rogue data cache load (CVE-2017-5754)

These vulnerabilities are commonly referred to as “Spectre” (variants 1 and 2) and “Meltdown” (variant 3). According to the Google Project Zero release, all three variants are the result of weaknesses in the implementation of out-of-sequence code execution also referred to as “speculative execution” or “branch prediction”, and exploitation requires the ability to run malicious code locally on the host. For more details please consult the following:

- https://googleprojectzero.blogspot.ca/2018/01/reading-privileged-memory-with-side.html
- https://spectreattack.com/spectre.pdf
- https://meltdownattack.com/meltdown.pdf

Affected Products:

None (see below for further details).

Details:

Sierra Wireless products are based on several different CPU architectures, some of which are affected by the vulnerabilities as noted in the following table. However, none of the products listed below allow execution of arbitrary code by an unauthorized user. Therefore, an attacker would first require the presence of a separate code injection vulnerability to exploit these issues and it is likely that an exploit of such a vulnerability would result in the compromise of the system without the need to exploit the Spectre or Meltdown vulnerabilities.

Embedded Solutions (Modules and Modems)		
Product	Vulnerability Exposure	Comments
N/A	None	No products use affected CPU architectures
Networking Solutions (Routers and Gateways)		
Product	Vulnerability Exposure	Comments
RV50	Spectre	Based on ARM Cortex-A9
MP70	Spectre	Based on ARM Cortex-A9
ACM	Spectre, Meltdown	Hardware appliance based on Intel Xeon; may also run on a guest OS within a virtualized environment (VMWare or AWS) that may be deployed on a vulnerable CPU architecture
AMM	Spectre, Meltdown	Hardware appliance based on Intel Xeon; may also run on a guest OS within a virtualized environment (VMWare or AWS) that may be deployed on a vulnerable CPU architecture
ALMS	Spectre, Meltdown	Runs on a guest OS within a virtualized environment (AWS) that may be deployed on a vulnerable CPU architecture
Cloud and Connectivity		
Product	Vulnerability Exposure	Comments
Airvantage	Spectre, Meltdown	Runs on a guest OS within a virtualized environment (AWS) that may be deployed on a vulnerable CPU architecture

Resolution:

RV50, MP70: No immediate action is required.

ACM, AMM Hardware appliance: No immediate action is required.

VMWare-deployed products (ACM, AMM): Customers are advised to contact VMWare and follow all recommended mitigation procedures for their VMWare instance.

AWS-deployed products (Airvantage, ALMS, ACM and AMM): No immediate action is required. AWS has already deployed mitigations for their infrastructure.

As part of a defense-in-depth strategy Sierra Wireless is evaluating kernel patches, CPU microcode updates and other mitigations for the products listed above and may deploy them as part of a future software update. Since some mitigation techniques are known to introduce significant performance impacts, Sierra Wireless will take the time to carefully test the impact of any mitigation on scalability before releasing updates.

Revision History

Revision	Date	Comments
1	2018-Jan-12	Initial Release

Further Information

For further information and technical support, please contact your authorized reseller or Sierra Wireless representative. To contact Sierra Wireless, please visit https://www.sierrawireless.com/company/contact-us/