IMPACT OF SPECTRE/MELTDOWN VULNERABILITIES IN ADI PRODUCTS

ADSA-2018-001

OVERVIEW

This advisory is in response to the January 3, 2018 public announcement (https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html) of the Spectre and Meltdown vulnerabilities recently found in hardware architectures and is intended for our customers to understand the impact of these vulnerabilities in Analog Devices and former Linear Technology (herein ADI) products. These vulnerabilities allow attackers to exploit design flaws that exist in certain processor-based products making use of local processor caching and speculative execution techniques. Upon release of these security vulnerabilities, ADI immediately began an analysis and investigation to determine how these vulnerabilities may impact our products. This advisory includes an enumeration of ADI products affected, details on the extent to which these products are affected, and suggested remediation that customers may take to mitigate the vulnerabilities. The information below represents our current and best efforts, and any additional updates from our findings will result in an update to this advisory.

INVESTIGATION

Our security and product teams have reviewed all generally available, nonevaluation, processor-based products from ADI, including both externally licensed and in-house developed processor cores. As a result of this investigation, we have not identified any generally available processor products to be vulnerable to the three variants defined in the References section.

We have identified a small number of system-level products with customer-specific installations that use local and public cloud-based environments. For these products, we are working directly with the affected customers to select and implement appropriate mitigations. Disclosure information regarding these customer-specific product installations are not detailed in this advisory.

DESCRIPTION

The Spectre and Meltdown vulnerabilities are categorized into three variants, each of which is based around the concept of speculative execution and how it functions with the cache in certain architectures. Combining these variants with a cache timing side-channel attack potentially allows an unprivileged application to access information outside of its intended execution context. Speculative execution exists in many modern processors as a performance enhancement mechanism to load data into the processor cache ahead of time, thus offsetting the memory access latency that would normally exist. Eventually the speculative execution engine will make a decision to either commit or discard the instructions that were executed speculatively, and in the latter case, revert the processor back to the expected state.

Additional detail for the Spectre variant vulnerabilities can be found at https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html and https://spectreattack.com/spectre.pdf.

Additional detail for the Meltdown variant vulnerability can be found at https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html and https://meltdownattack.com/meltdown.pdf.

REFERENCES

Additional details in reference to this disclosure can be found at:

- https://spectreattack.com/spectre.pdf
- https://meltdownattack.com/meltdown.pdf
- https://developer.arm.com/support/security-update
- https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

This disclosure is in response to the following CVEs.

CVE Identifier	Links
CVE-2017-5753	https://nvd.nist.gov/vuln/detail/CVE-2017-5753
CVE-2017-5715	https://nvd.nist.gov/vuln/detail/CVE-2017-5715
CVE-2017-5754	https://nvd.nist.gov/vuln/detail/CVE-2017-5754

REVISION HISTORY

Date	Change Log
1/30/2018	▶ Initial Publication

CONTACT INFORMATION

Analog Devices wants to ensure our customers are successful in development of their applications using the products mentioned. For support or questions regarding the above information, please contact:

- Your field sales and application engineers
- Your local franchise distributors (analog.com/sales)
- ADI technical support (form.analog.com/form_pages/support/integrated/techsupport.aspx)

Analog Devices is committed to ensuring the security of our product offerings. To report potential security issues on Analog Devices' products, please contact securityalert@analog.com or your local technical support resource.