Speculative Execution Data Cache And Indirect Branch Prediction Method Side Channel Analysis Advisory

Intel ID:	INTEL-OSS-10003
Product family:	Most Modern Operating Systems
Imact of vulnerability:	Information Disclosure
Severity rating:	Important
Original release:	01/03/2018
Last revised:	01/03/2018
CVE:	CVE-2017-5754

SUMMARY

Today a team of security researchers disclosed several software analysis methods that, when used for malicious purposes, have the potential to improperly gather sensitive data from many types of computing devices with many different vendors' processors and operating systems.

Intel is committed to product and customer security and to responsible disclosure. We worked closely with many other technology companies, including AMD, ARM Holdings and several operating system vendors, to develop an industry-wide approach to mitigate this issue promptly and constructively.

For facts about these new exploits, and steps you can take to help protect your systems and information please visit: https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html.

DESCRIPTION

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.

AFFECTED PRODUCTS

Most modern operating systems are impacted. Intel recommends checking with your Operating System Vendor(s) for updates or patches.

RECOMMENDATIONS

Along with other companies whose platforms are potentially impacted by these new methods, including AMD and ARM, Intel has worked with operating system vendors, equipment manufacturers, and other ecosystem partners to develop software updates that can help protect systems from these methods. End users and systems administrators should check with their operating system vendors and apply any available updates as soon as practical.

ACKNOWLEDGEMENTS

Intel would like to thank Jann Horn with Google Project Zero for his original report and for working with the industry on coordinated disclosure.

Intel would also like to thank the following researchers for working with us on coordinated disclosure.

- Moritz Lipp, Michael Schwarz, Daniel Gruss, Stefan Mangard from Graz University of Technology
- Paul Kocher, Daniel Genkin from University of Pennsylvania and University of Maryland, Mike Hamburg from Rambus, Cryptography Research Division and Yuval Yarom from University of Adelaide and Data61.
- Thomas Prescher and Werner Haas from Cyberus Technology, Germany

*Originally published by 01.org