Speculative Execution Branch Prediction Side Channel And Branch Prediction Analysis Method Advisory

Intel ID:	INTEL-OSS-10002
Product family:	Most Modern Operating Systems
Impact of vulnerability:	Information Disclosure
Severity rating:	Important
Original release:	01/03/2018
Last revised:	07/10/2018
CVE:	CVE-2017-5753, CVE-2018-3693

SUMMARY

On January 3, 2018, 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.

On Jul 10, 2018, additional research disclosed related variations of these methods.

Protecting our customers' data and ensuring the security of our products is a top priority for Intel and we will continue to work with customers, partners and researchers to understand and mitigate any vulnerabilities that are identified.

DESCRIPTION

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.
- 7.1 High CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

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.
- 7.1 High CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

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 or developer guidance 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

BOUNDS CHECK BYPASS - CVE-2017-5753

- 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

BOUNDS CHECK BYPASS STORE - CVE-2018-3693

- Intel would like to thank Vladimir Kiriansky (MIT) and Carl Waldspurger (Carl Waldspurger Consulting) for reporting and for working with the industry on coordinated disclosure.
- Intel would also like to thank employees Kekai Hu, Ke Sun, Henrique Kawakami and Rodrigo Branco

*Originally published by 01.org