INTEL-SA-00088

# THE LATEST SECURITY INFORMATION ON INTEL® PRODUCTS.



## Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method

| | |
|---|---|
| Product family | Systems with Speculative Execution |
| Impact of vulnerability | Information Disclosure |
| Severity rating | Important |
| Original release | Jan 03, 2018 |
| Last revised | July 22, 2019 |

**Summary:**

**Updated Recommendations Section 04/04/2018**

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.

› 5.6 Medium CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

**Affected products:**

- For non-Intel based systems please contact your system manufacturer or microprocessor vendor (AMD, ARM, Qualcomm, etc.) for updates.

The following Intel-based platforms are impacted by this issue. Intel may modify this list at a later time. Please check with your system vendor or equipment manufacturer for more information regarding updates for your system.

- Intel® Core™ i3 processor (45nm and 32nm)
- Intel® Core™ i5 processor (45nm and 32nm)
- Intel® Core™ i7 processor (45nm and 32nm)
- Intel® Core™ M processor family (45nm and 32nm)
- 2nd generation Intel® Core™ processors
- 3rd generation Intel® Core™ processors
- 4th generation Intel® Core™ processors
- 5th generation Intel® Core™ processors
- 6th generation Intel® Core™ processors
- 7th generation Intel® Core™ processors
- 8th generation Intel® Core™ processors
- Intel® Core™ X-series Processor Family for Intel® X99 platforms
- Intel® Core™ X-series Processor Family for Intel® X299 platforms
- Intel® Xeon® processor 3400 series
- Intel® Xeon® processor 3600 series
- Intel® Xeon® processor 5500 series
- Intel® Xeon® processor 5600 series
- Intel® Xeon® processor 6500 series
- Intel® Xeon® processor 7500 series
- Intel® Xeon® Processor E3 Family

- Intel® Xeon® Processor E3 v2 Family
- Intel® Xeon® Processor E3 v3 Family
- Intel® Xeon® Processor E3 v4 Family
- Intel® Xeon® Processor E3 v5 Family
- Intel® Xeon® Processor E3 v6 Family
- Intel® Xeon® Processor E5 Family
- Intel® Xeon® Processor E5 v2 Family
- Intel® Xeon® Processor E5 v3 Family
- Intel® Xeon® Processor E5 v4 Family
- Intel® Xeon® Processor E7 Family
- Intel® Xeon® Processor E7 v2 Family
- Intel® Xeon® Processor E7 v3 Family
- Intel® Xeon® Processor E7 v4 Family
- Intel® Xeon® Processor Scalable Family
- Intel® Xeon Phi™ Processor 3200, 5200, 7200 Series
- Intel® Atom™ Processor C Series
- Intel® Atom™ Processor E Series
- Intel® Atom™ Processor A Series
- Intel® Atom™ Processor x3 Series
- Intel® Atom™ Processor Z Series
- Intel® Celeron® Processor J Series
- Intel® Celeron® Processor N Series
- Intel® Pentium® Processor J Series
- Intel® Pentium® Processor N Series

**Recommendations:**

**Updated 04/04/2018**

Intel has worked with operating system vendors, equipment manufacturers, and other ecosystem partners to develop platform firmware and software updates that can help protect systems from these methods.

This includes the release of updated Intel microprocessor microcode to our customers and partners. Details can be found here: http://newsroom.intel.com/microcode

End users and systems administrators should check with their OEM and system software vendors and apply any available updates as soon as practical.

For non-Intel based systems please contact your system manufacturer or microprocessor vendor (AMD, ARM, Qualcomm, etc.) for updates.

Other variants of this side-channel analysis are being addressed by Operating System and Software Vendors. For more details see:

- CVE-2017-5753
- CVE-2017-5754

**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
- Kekai Hu, Ke Sun, Henrique Kawakami, Rodrigo Branco from Intel

# Revision history:

| Revision | Date | Description |
|---|---|---|
| 1.0 | 03-January-2018 | Initial Release |
| 1.1 | 03-January-2018 | Update Links |
| 1.2 | 05-January-2018 | Update |
| 1.3 | 09-January-2018 | Update |
| 1.4 | 10-January-2018 | New Link |
| 1.5 | 17-January-2018 | Status update |
| 1.6 | 22-January-2018 | Status Update |
| 1.7 | 27-January-2018 | Rec Update |
| 1.8 | 02-February-2018 | Rec Update |
| 1.9 | 20-February-2018 | Rec Update |
| 2.0 | 04-April-2018 | Rec Update |
| 2.1 | 14-March-2019 | CVSS correction |
| 2.2 | 22-July-2019 | Updated Acknowlegements |

**CVE Name:** CVE-2017-5715

## Legal Notices and Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as

errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.



Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at https://intel.com .

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.



## Report a Vulnerability

If you have information about a security issue or vulnerability with an **Intel branded product or technology**, please send an e-mail to secure@intel.com . Encrypt sensitive information using our PGP public key .

Please provide as much information as possible, including:

- The products and versions affected
- Detailed description of the vulnerability
- Information on known exploits

A member of the Intel Product Security Team will review your e-mail and contact you to collaborate on resolving the issue. For more information on how Intel works to resolve security issues, see:

- Vulnerability handling guidelines

For issues related to Intel's external web presence (Intel.com and related subdomains), please contact Intel's External Security Research team.

## Need product support?

The secure@intel.com e-mail address should only be used for reporting security issues.



If you...

- Have questions about the security features of an Intel product
- Require technical support
- Want product updates or patches

Please visit Support & Downloads .

USA (English)