






INTEL-SA-00145

THE LATEST SECURITY INFORMATION ON INTEL[®] PRODUCTS.

[Report a Vulnerability](#) [Product Support](#)

LAZY FP STATE RESTORE

Intel ID:	INTEL-SA-00145	USA (English)   
Product family:	Intel® Core-based microprocessors.	
Impact of vulnerability:	Information Disclosure	
Severity rating:	Moderate	
Original release:	06/13/2018	
Last revised:	07/23/2019	

Summary:

System software may utilize the Lazy FP state restore technique to delay the restoring of state until an instruction operating on that state is actually executed by the new process. Systems using Intel® Core-based microprocessors may potentially allow a local process to infer data utilizing Lazy FP state restore from another process through a speculative execution side channel.

Description:

System software may opt to utilize Lazy FP state restore instead of eager save and restore of the state upon a context switch. Lazy restored states are potentially vulnerable to exploits where one process may infer register values of other processes through a speculative execution side channel that infers their value.

- CVSS - 4.3 Medium CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Affected Products:

Intel® Core-based microprocessors.

Recommendations:

If an XSAVE-enabled feature is disabled, then we recommend either its state component bitmap in the extended control register (XCR0) is set to 0 (e.g. XCR0[bit 2]=0 for AVX, XCR0[bits 7:5]=0 for AVX512) or the corresponding register states of the feature should be cleared prior to being disabled. Also for relevant states (e.g. x87, SSE, AVX, etc.), Intel recommends system software developers utilize Eager FP state restore in lieu of Lazy FP state restore.

Acknowledgements:

Intel would like to thank Julian Stecklina from Amazon Germany, Thomas Prescher from Cyberus Technology GmbH (<https://www.cyberus-technology.de/>), Alex Zuepke, Rudolf Marek and Zdenek Sojka from SYSGO AG (<http://sysgo.com>), Colin Percival and for reporting this issue and working with us on coordinated disclosure.

Intel would also like to thank employees Kekai Hu, Ke Sun, Henrique Kawakami and Rodrigo Branco for CVE-2018-3665.

Revision History

Revision	Date	Description
1.0	06/13/2018	Initial Release
1.1	07/23/2019	Updated Acknowledgements

CVE Name: CVE-2018-3665

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.



USA (English)   

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © Intel Corporation 2019

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 security issues.

e-mail address should only be used for reporting

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)   

[Company Information](#)

[Our Commitment](#)

[Communities](#)

[Investor Relations](#)

[Contact Us](#)

[Newsroom](#)

[Jobs](#)



© Intel Corporation

[Terms of Use](#)

[*Trademarks](#)

[Privacy](#)

[Cookies](#)

[Supply Chain Transparency](#)

