intel newsroom

All News ▾ Search Newsroom...

Editorial

August 14, 2018

Contact Intel PR

By Leslie Culbertson

Intel's Product Assurance and Security (IPAS) team is focused on the cybersecurity landscape and constantly working to protect our customers. Recent initiatives include the expansion of our Bug Bounty program and increased partnerships with the research community, together with ongoing internal security testing and review of our products. We are diligent in these efforts because we recognize bad actors continuously pursue increasingly sophisticated attacks, and it will take all of us working together to deliver solutions.

Today, Intel and our industry partners are sharing more details and mitigation information about a recently identified speculative execution side-channel method called L1 Terminal Fault (L1TF). This method affects select microprocessor products supporting Intel® Software Guard Extensions (Intel® SGX) and was first reported to us by researchers at KU Leuven University*, Technion – Israel Institute of Technology*, University of Michigan*, University of Adelaide* and Data61*[1]. Further research by our security team identified two related applications of L1TF with the potential to impact other microprocessors, operating systems and virtualization software.

More: Security Exploits and Intel Products (Press Kit) | Security Research Findings (Intel.com)

I will address the mitigation question right up front: Microcode updates (MCUs) we released earlier this year are an important component of the mitigation strategy for all three applications of L1TF. When coupled with corresponding updates to operating system and hypervisor software released starting today by our industry partners and the open source community, these updates help ensure that consumers, IT professionals and cloud service providers have access to the protections they need.

L1TF is also addressed by changes we are already making at the hardware level. As we announced in March, these changes begin with our next-generation Intel® Xeon® Scalable processors (code-named Cascade Lake), as well as new client processors expected to launch later this year.

We are not aware of reports that any of these methods have been used in real-world exploits, but this further underscores the need for everyone to adhere to security best practices. This includes keeping systems up-to-date and taking steps to prevent malware. More information on security best practices is available on the Homeland Security website.

About L1 Terminal Fault

All three applications of L1TF are speculative execution side channel cache timing vulnerabilities. In this regard, they are similar to previously reported variants. These particular methods target access to the L1 data cache, a small pool of memory within each processor core designed to store information about what the processor core is most likely to do next.

The microcode updates we released earlier this year provide a way for system software to clear this shared cache. Given the complexity, we created a short video to help explain L1TF.

Once systems are updated, we expect the risk to consumer and enterprise users running *non-virtualized* operating systems will be low. This includes most of the data center installed base and the vast majority of PC clients. In these cases, we haven't seen any meaningful performance impact from the above mitigations based on the benchmarks we've run on our test systems.

There is a portion of the market – specifically a subset of those running traditional virtualization technology, and primarily in the data center – where it may be advisable that customers or partners take additional steps to protect their systems. This is principally to safeguard against situations where the IT administrator or cloud provider cannot guarantee that all virtualized operating systems have been updated. These actions may include enabling specific hypervisor core scheduling features or choosing not to use hyper-threading in some specific scenarios. While these additional steps might be applicable to a relatively small portion of the market, we think it's important to provide solutions for all our customers.

For these specific cases, performance or resource utilization on some specific workloads may be affected and varies accordingly. We and our industry partners are working on several solutions to address this impact so that customers can choose the best option for their needs. As part of this, we have developed a method to detect L1TF-based exploits during system operation, applying mitigation only when necessary. We have provided pre-release microcode with this capability to some of our partners for evaluation, and hope to expand this offering over time.

For more information on L1TF, including detailed guidance for IT professionals, please visit the advisory on the security center. We've also provided a white paper and updated the FAQs on our security first website.

I'd like to again thank our industry partners and the researchers who first reported these issues for their collaboration and collected commitment to coordinated disclosure. Intel is committed to the security assurance of our products, and will continue to provide regular updates on issues as we identify and mitigate them.

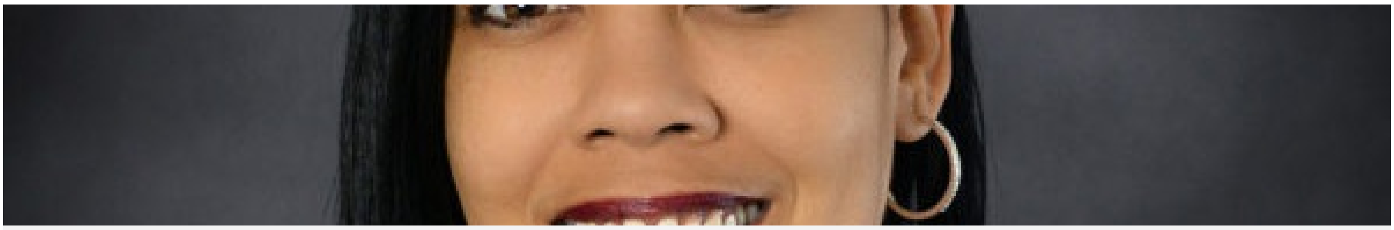
As always, we continue to encourage everyone to take advantage of the latest security protections by keeping your systems up-to-date.

Leslie Culbertson is executive vice president and general manager of Product Assurance and Security at Intel Corporation.

[1] Raoul Strackx, Jo Van Bulck, Marina Minkin, Ofir Weisse, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Thomas F. Wenisch, and Yuval Yarom

Tags: IPAS, Leslie Culbertson

Other News



April 14, 2021
Intel Names Dawn Jones CDIO and VP of Social Impact

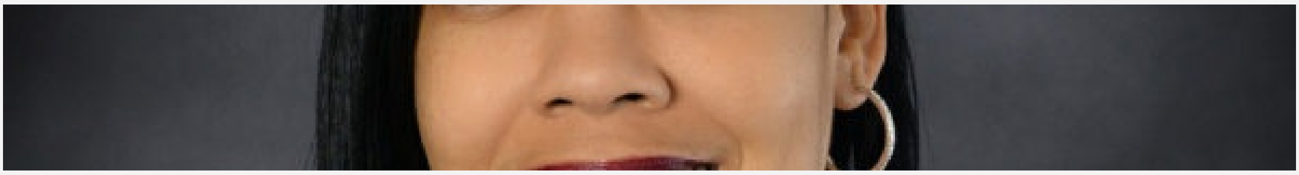
April 7, 2021
Media Alert: April Intel Partner Connect 2021 (Virtual)

April 6, 2021
Intel Xeon Advances Nasdaq's Homomorphic Encryption R&D

About Intel

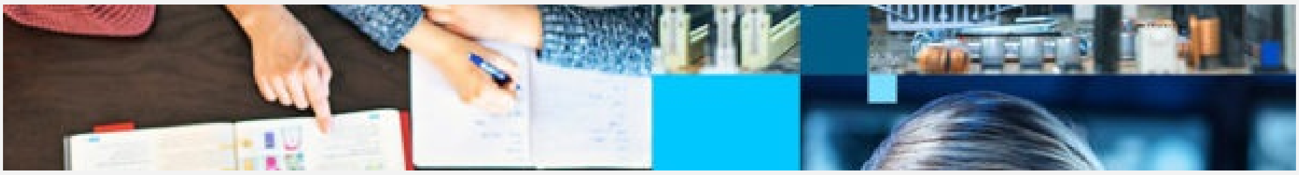
Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

Latest News: Corporate



April 14, 2021
Intel Names Dawn Jones CDIO and VP of Social Impact

April 7, 2021
Media Alert: April Intel Partner Connect 2021 (Virtual)



April 7, 2021
Leveraging Technology to Provide Global Pandemic Relief

Read More