Spectre and Meltdown Vulnerabilities

Researchers have recently discovered Spectre (CVE-2017-5715/CVE-2017-5753) and Meltdown (CVE-2017-5754) vulnerabilities in multiple microprocessors that use speculative execution. These vulnerabilities allow an attacker with existing execution access to potentially deduce the contents of memory across security boundaries which they would otherwise not be able to access. In particular, an attacker with user-level execution capabilities may be able to utilize these attacks to access memory in other processes, the OS kernel, virtual machines, and hypervisor memory. Mitigations to such attacks are currently being implemented in multiple processor microcode updates and within multiple operating systems.

Overview

- Both Spectre and Meltdown are able to be used to read memory regions that a user should not be able to access. That could include access to memory in other processes, virtual machines, hypervisor memory, and even the OS kernel. These memory regions possibly contain sensitive information such as passwords, encryption keys, or proprietary information. These are read-only vulnerabilities and do not enable modifying those restricted memory regions.
- Spectre and Meltdown do not provide a means to access a system or execute code. The attacker must either exploit some other system vulnerability to gain access or convince an authorized user to run malware containing the Spectre or Meltdown attack. Note that this malware does not need to be installed on the system but may be JavaScript code executed from a remote source.

Affected Processors in Mercury Systems

- Multiple generations of Intel CPUs going back to 2011 and in some cases further, are vulnerable to both Spectre and Meltdown. For example, this includes Core i5, Core i7, Xeon D, Xeon EP, Xeon SP, and some Atom processors. A full list of Intel processors that are affected is available in the Intel Security Advisory INTEL-SA-00088.
- Mercury product lines that use the affected Intel processors include Ensemble™ 3000, 5000, 6000, 8000, and 9000 Series, as well as BuiltSAFE™ SBCs using Core i7 processors.
- Certain NXP processors are vulnerable to Spectre, including those using e500mc and e5500 cores. Example processors used in Mercury's BuiltSAFE™ SBCs include P2010, P2020, P2080, P3041, P4080, and P5020.

Mitigations

It is possible to fully mitigate the impact of Meltdown by installing updates to the operating system (OS) and any applicable hypervisor. Spectre vulnerabilities are only partially mitigated by such updates. Mitigation for one variant of Spectre also requires a processor microcode update in the BIOS. Some of these mitigations may have a noticeable performance impact that varies with syscall rate, page fault rate, and working set size (which drives to TLB flushing). As a result, customers need to evaluate the security posture of their system to see if the patches effectively increase operational security (OPSEC).

Many military embedded systems maintain tight process control over their trusted computing base, restrict access to source and binary code, and do not run a web server or any other run-time compliers and interpreters that could be used to execute arbitrary code. The OPSEC of such systems severely limits the risk of Meltdown and Spectre.

Mercury customers who have deployed the full suite of Mercury's BuiltSECURE™ technology together with the StarLab's Crucible® hypervisor are architecturally protected from this class of attack. The BuiltSECURE suite includes additional authentication of BIOS and applications as part of a secure boot and secure runtime environment, giving customers built-in control to prevent unauthentic malware that could be used to execute arbitrary code. When Crucible® is configured such that each virtual machine is bound to a different processor core it provides another layer of protection against runtime memory attacks. Customers are encouraged to contact their Mercury account manager to see if their particular Ensemble products can be upgraded with the full suite of BuiltSECURE technology.

Patches

Customers interested in applying patches for Spectre and Meltdown are encouraged to contact Mercury Customer Support for assistance so that Mercury may be able to tailor the solution to such customer's specific program requirements.

Alternatively, customers who purchased OS licenses identified below directly from the OS companies may also be able to download patches from those supplier sites. In such an instance, such customer will need to rebuild the Mercury drivers against the new kernel.

Redhat: RHEL 7, RHEL 6, RH5

VxWorks: 7, 6.x