Intel CPU Security Vulnerabilities: Spectre, Meltdown

Product Name
Fiery Controllers

Affects Version
See the Description and Details for affected products

Description
EFI is aware of the recently discovered vulnerabilities, Meltdown and Spectre, which allow applications to access secure data due to recently discovered fundamental microprocessor design flaws. Per The Register's 1/2/2018 article, Meltdown and Spectre are the result of "a fundamental design flaw in Intel's processor." The Register goes on to report that the processor design flaw "has forced a significant redesign of the Linux and Windows kernels to defang the chip-level security bug."
Source: https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/
There are 3 CVEs associated with the issues:

1. CVE-2017-5753: bounds check bypass (Also called Spectre)
2. CVE-2017-5715: branch target injection (Also called Spectre)
3. CVE-2017-5754: rogue data cache load (also called Meltdown)

https://meltdownattack.com/ has a good explanation of Meltdown and Spectre.

1. **Meltdown** allows any application to access all system memory, including memory allocated for the kernel. Mitigation for this vulnerability will require operating system patches and potentially firmware updates. Patches for this vulnerability may have a performance impact on systems. **So far, only Intel chips have been shown to be vulnerable.**
2. **Spectre** allows an application to force another application to access arbitrary portions of its memory, which can then be read through a side channel. This vulnerability may require changes to processor architecture in order to fully mitigate. **According to Google Project Zero, this vulnerability impacts Intel, AMD, and ARM chips.**

Detail
Affected Fiery Systems:

- Fiery servers running Windows OS

Is there a fix/workaround and can it be applied to Fiery controllers?
Patches have been developed by Microsoft and Apple developers for protection against Meltdown for Windows (7, 8.1, & 10) and OS X. Efforts are also in progress that focus on hardening software against future exploitation of Spectre, respectively to patch software after exploitation through Spectre (LLVM patch, ARM speculation barrier header).

For Windows-based Fiery controllers, EFI will be conducting testing with the fixes that are developed as they are made publicly available. EFI evaluation of some of these fixes is already under way.

Note: Our Linux-based Fiery controllers are enclosed systems, and it is not possible for a user to access the system in a way that would allow installation of programs that would expose this vulnerability.

Please make sure that the patches indicated below are installed. These patches are Windows updates distributed by Microsoft:

Operating System	Microsoft Fix
Win7 SP1	KB4056894
Win 8.1	KB4056895
Win10	KB4056890

A Bios fix to complete the scope of both Spectre vulnerabilities is still in progress. EFI is currently evaluating the solution from Intel. EFI will communicate the BIOS schedule for each HW platform when it is available.

EFI recommends to periodically check our EFI Smart Support public knowledgebase for the latest info/status on this issue.

http://www.efi.com/support-and-downloads/kbarticle/article-details/?knowledgeArticleID=kA339000000HCDaCAO

Please contact your EFI Program Manager for additional information.