Is EFT affected by the recent "Meltdown" and "Spectre" vulnerabilities?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT™ all versions
- EFT Arcus

QUESTION

Is EFT affected by the "Meltdown" and "Spectre" vulnerabilities? If exploited, can attackers gain access to protected information stored in memory? And if patched, what is the impact to performance?

ANSWER

No, EFT itself is not directly affected by the Meltdown or Spectre vulnerabilities. Instead, it they are vulnerabilities affecting hardware components of computers on which EFT runs. However, because vulnerabilities that affect the underlying infrastructure could pose a risk to sensitive data used by EFT, Globalscape does have advice for customers.

Globalscape's advice to our customers is that they urgently apply the appropriate operating system (OS) and/or firmware patches to mitigate Spectre and Meltdown attacks. The threat vectors of these vulnerabilities involve running potentially malicious applications on the same machine (physical machine, not just the virtual machine in which EFT operates) which can leverage speculative execution to do side-channel attacks on the cache to steal memory-based information. At some point, EFT necessarily has sensitive information in memory (user login credentials, key materials, file contents, etc.) for very short periods. Even if EFT securely wiped the data in memory (which EFT does key materials, but not for file contents that are streamed through the network stack to disk, but require at least a block of data in memory at any time, between 4K and 64K of data), there are short periods where sensitive data would be exposed, such as immediately upon receiving a login password for an incoming session, and prior to hashing the password in order to perform a lookup.

Aside from patching vulnerable systems, Globalscape's advice is that customers ensure that only trusted applications can run on the physical hardware on which EFT is running. This means patched Windows OS, trusted third-party applications, services, and drivers (SQL Server or Oracle databases; Windows File Share; etc). Furthermore, customers should ensure that no custom commands nor AWE task executions invoke untrusted third-party

applications or scripts. Lastly, customers should not use other applications on the server (Web browsers, office productivity tools, etc.), retaining a “single role” which further limits potential attack vectors. Globalscape's software itself does not execute code unless directed by the configuration (custom commands, AWE tasks) of the server. Therefore, as long as the physical machine on which EFT is running is patched and has known good software running atop it, the risk of Meltdown or Spectre attacks revealing sensitive information is reduced as much as possible.

What about the impact on performance for patched systems? Assessing performance impact is complicated, and highly dependent on your hardware, OS, and workload. Globalscape recommends that customers check with their hardware vendor to assess potential performance impact and mitigation techniques. Depending upon workloads, reports from the industry indicate somewhere between 3% and 30%. Globalscape recommends that customers run on the latest available stable OS to ensure minimal performance loss; however the actual performance impact is heavily dependent upon the deployment and usage patterns of the EFT server, and we recommend that customers review performance characteristics after applying OS updates to ensure appropriate service levels are being met. If services levels fall beneath desired threshold, then customers may want to consider scaling out their EFT deployment with an Active-Active cluster as a way of ensuring high service levels even when any individual machine has performance degradation caused by Spectre and Meltdown patches.

EFT Arcus

EFT Arcus customers were unaffected. Microsoft Azure accelerated their normal planned maintenance schedule and applied the appropriate updates on January 3rd. The majority of Azure customers should not see a noticeable performance impact with this update. Azure has worked to optimize the CPU and disk I/O path and Azure customers are not seeing noticeable performance impact after the fix has been applied. This Azure infrastructure update addresses the disclosed vulnerability at the hypervisor level and does not require an update to your Windows or Linux VM images.

For more information,
visit https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11400/Is-EFT-affected-by-the-recen...