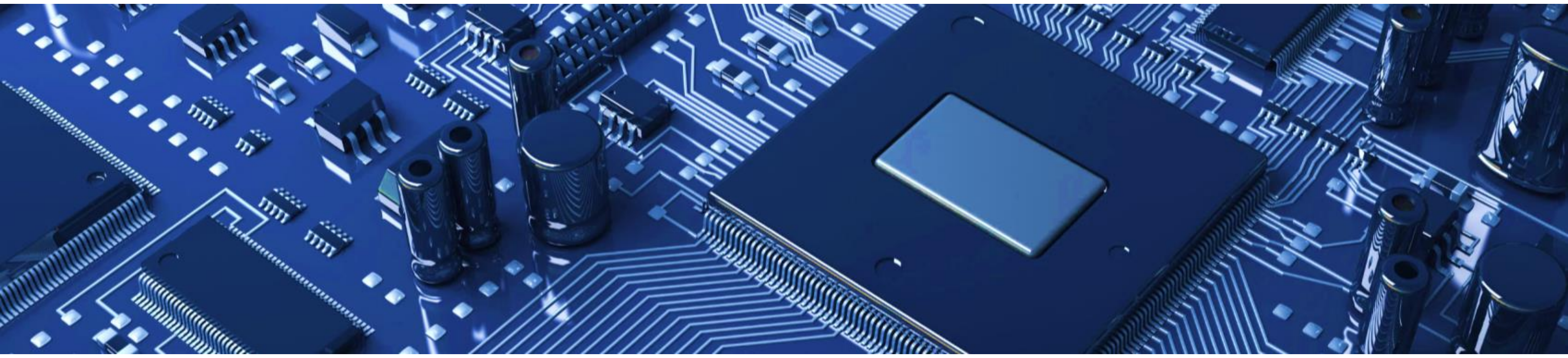
TECHNICAL NOTE



# Mitigating the Performance Penalty of Spectre and Meltdown

## Processor design flaws create vulnerabilities to hacking, and the patches cause performance impacts

### The Details You Need To Know

Two new security vulnerabilities were revealed on January 3rd 2018, that open the door for hackers to access sensitive system data. The flaws, known as Spectre and Meltdown, impact the CPUs of systems ranging from phones to servers and the existence of the problems may go back more than two decades. The flaw relates to a common design practice that is employed by most modern processor designers. While patches are available from major chip and OS vendors, applying these patches can have a major impact on system performance. This can be avoided by deploying SmartNIC technologies that offload processing from the CPU by shouldering the burden of processing the TCP/IP and storage network stacks. Adapters that deploy network "OnLoad" technologies do exactly the opposite – burdening the CPU with networking functions that rob horsepower from business applications. As a result, many common workloads such as OLTP, database analytics and virtual machines are susceptible to performance impacts on servers that have been patched.

### How To Protect Against Spectre and Meltdown

Patches against both attacks are available from operating system, virtual machine vendors, and for Linux distributions, while operating system kernel and firmware updates are also available. A comprehensive list of devices affected along with associated patches issued by vendors can be found on a single website from European Research Council (ERC).

### KEY TAKEAWAYS

- Most modern processors are affected and are vulnerable to Spectre and Meltdown attacks
- Patches to fix Spectre and Meltdown have shown performance degradation across most workloads
- Networking Offload technologies have demonstrated minimal to no degradation of performance

### Vendor Warnings

Microsoft recommends evaluating the risk of patching versus performance tradeoff.

VMware has warned that applying fixes will result in an increase of CPU utilization that may result in insufficient capacity.

## How Patching Will Affect Computers

The nature of the flaws means that fixes to guard against attacks have the effect of slowing down computers and can cause a significant decrease in server performance. The worst affected workloads were those "that incorporate a larger number of user/kernel privilege changes and spend a significant amount of time in privileged mode", according to Intel.

Analysis by Mellanox (Fig. 1) of system performance affected by applying fixes found the following:

- Benchmarks to simulate common enterprise and cloud workloads saw between 2 – 5 % negative performance impact.
- Database analytics and Java VM benchmarks showed a 3 – 7%  performance impact
- OLTP benchmark simulating models similar to a brokerage firm showed a 8 – 19% impact.
- Accelerator technologies including DPDK, RDMA and others  demonstrated minimal to no degradation of performance.

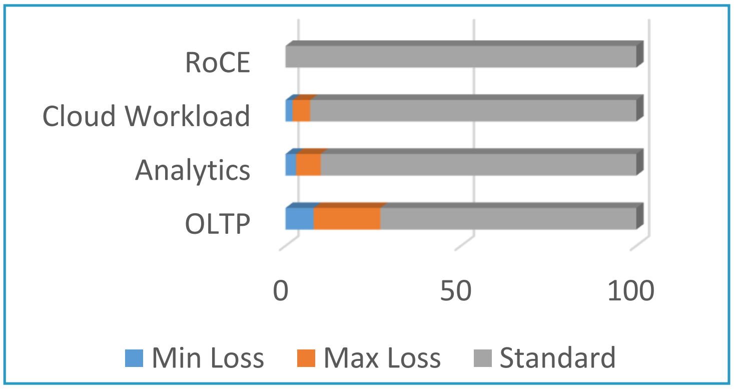


**Fig. 1  Average Performance Loss After Patching**

## Offload Interconnects Alleviate Performance Loss

Mellanox delivers offload technologies such as RDMA and DPDK to remove the burden of processing  the TCP/IP and storage stacks from the main system processor, moving it to the network adapter. This provides performance advantages and alleviates performance losses typically seen when patching systems for Spectre and Meltdown (Fig2).

Adapters that utilize basic onload technologies must rely on the CPU to process the TCP/IP stack and negatively impact systems that are patched. Performance testing on systems that are affected before and after applying patches were found to have a performance loss of up to 47 percent (Fig. 3).

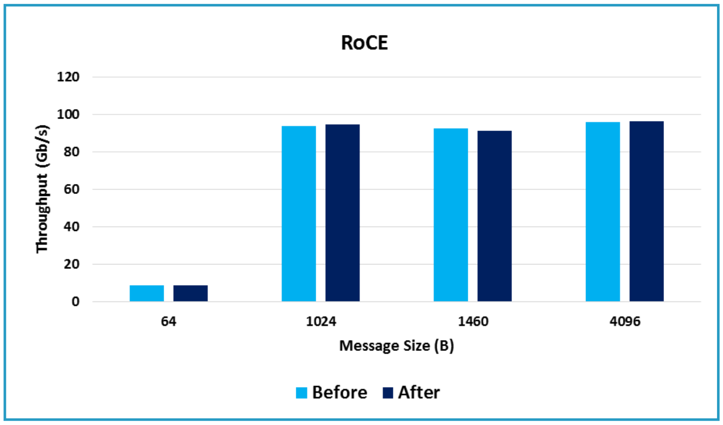


**Fig. 2 RoCE Performance Impact: 0%**

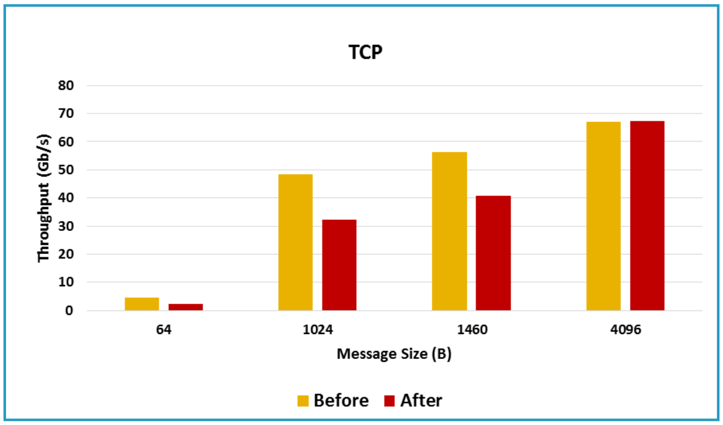


**Fig .3  Without RoCE Performance Impact: - 47%**

## Conclusion

Reports of serious performance implications for systems with patches range from 5% - 30%. Internal testing by Mellanox found a similar range from 2%  - 47%. This will have a huge impact on large data centers in both OpEx and CapEx as servers will need to be replaced or additional servers added to compensate for the performance losses. This presents a more compelling case than ever to utilize server “offload” technologies that are available with Mellanox network adapter and switches.

**Learn More:**

Interconnect Performance Evaluation