Cisco Contact Center Performance Impacts from Side-Channel Information Disclosure Vulnerabilities

Under normal conditions, the Unified Contact Center Enterprise (UCCE) Team has instructed customers to assess and apply Microsoft security updates as they see fit. Here is our excerpted policy from the link below:
https://www.cisco.com/c/en/us/products/collateral/customer-collaboration/unified-contact-center-enterprise/product_bulletin_c25-455396.html
"Customers are responsible for reviewing any security update released by Microsoft for Windows, IIS, and SQL Server, and assessing their security exposure to the vulnerability. If deemed necessary, customers should follow Microsoft's guidelines to apply these updates to the relevant systems as soon as possible."

Recent microprocessor side-channel vulnerabilities have been publicized in the media, dubbed "Meltdown" and "Spectre". The Cisco impact is described in a PSIRT Advisory here:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180104-cpusidechannel

Because the root cause of these issues is the microprocessor design, a hardware fix is not practical. As a result, software and firmware updates from the vendors of the microprocessor, hardware, operating systems, and hypervisor are becoming available.

The primary concern with these fixes is that they may reduce processor performance, impacting Contact Center capacity. Intel has stated[1] that the processing impacts are workload dependent and initial testing[2] has shown little performance impact, but there have also been reports[3] that the impact could range from 5-30%, leading to customer concerns.

Cisco performance testing of Contact Center solutions with the available fixes shows a 2-5% increase in disk IOPS[4], as well as a reduction in memory page usage. These changes are not significant enough to require restructuring of the VM definitions or capacity changes.

Notes:
1) https://newsroom.intel.com/news-releases/industry-testing-shows-recently-released-security-updates-not-impacting-performance-real-world-deployments/
2) https://newsroom.intel.com/news-releases/industry-testing-shows-recently-released-security-updates-not-impacting-performance-real-world-deployments/
3) https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/
4) https://blogs.technet.microsoft.com/srd/2018/03/23/kva-shadow-mitigating-meltdown-on-windows/