



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

Under normal conditions, the Cisco® Unified Contact Center Enterprise (UCCE) Team has instructed customers to assess and apply Microsoft security updates as they see fit. Here is an excerpt of our 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 microprocessors, hardware, operating systems, and hypervisors are becoming available.

The primary concern with these fixes is that they may reduce processor performance, impacting contact center capacity. Intel has stated¹ that the processing impacts are workload dependent and that initial testing² has shown little performance impact, but there have also been reports³ that the impact could range from 5 to 30 percent, leading to customer concerns.

Cisco's performance testing of contact center solutions with the available fixes shows a 2 to 5 percent 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/>




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)