

Spectre and Meltdown Compute Capacity Relief FAQs

What is the concern?

On January 3, 2018, the **National Cybersecurity and Communications Integration Center** (NCCIC) became [aware](#) that some CPU hardware implementations are vulnerable to a class of security vulnerabilities called “side-channel attacks,” referred to as Meltdown and Spectre: CVE-2017-5715 (Spectre), CVE-2017-5753 (Spectre), and CVE-2017-5754 (Meltdown).

What is the impact?

Per NCCIC, an attacker could exploit these hardware security vulnerabilities to gain unauthorized access to arbitrary in-memory data, potentially including sensitive or privileged information processed on an affected computer. Also per NCCIC, *“after patching, performance may be diminished by **up to 30 percent**. Administrators should ensure that performance is monitored for critical applications and services, and work with their vendor(s) and service provider(s) to mitigate the effect if possible.”*

What steps are being taken by the industry to address the situation?

Per NCCIC, operating system (OS)-level patches have been made available to work around these hardware vulnerabilities. Cloud service providers have applied these OS patches to their systems. Per NCCIC, *“after [OS] patching, [application] performance may be diminished by **up to 30 percent**.”*

What specifically is Informatica doing about it?

These potential performance impact issues are **not unique to Informatica**—but they do affect how Informatica’s software runs on servers and cloud systems. Informatica is pursuing all appropriate actions to assure the protection of Informatica’s systems and services against these vulnerabilities including: accelerating Informatica’s regular patching program to patch all systems and software as updates are made available from manufacturers and our supply chain partners; and, evaluating and mitigating possible system, software, and cloud performance impacted by these vulnerabilities

- **For Informatica’s on-premises customers** concerned about hardware capacity lost as a result of applying OS-level patches, Informatica’s R&D teams have performance testing underway.
 - As we complete our evaluation, we will provide additional guidance via <https://network.informatica.com>. Customers concerned with the potential impact to their hardware capacity should contact Informatica **Global Customer Support** (GCS) for a temporary increase in licensed CPU-cores while they evaluate these OS patches.
- **For Informatica’s cloud customers** that may be concerned about OS patches applied in a timely manner to mitigate the security concerns, Informatica’s R&D teams have OS patching underway.
 - We are working closely with our infrastructure partners to update systems consistent with our internal security standards. We expect minimal customer impact while we apply patches to our cloud services; scheduled maintenance activities will be posted to <https://status.informatica.com>.

What specifically does a customer receive from Informatica?

Informatica is providing a temporary increase of up to 30 percent more compute capacity at no charge for 30 days from the time the customer's request is granted by Informatica, for all customers of applicable Informatica products, as they figure out how much extra compute capacity they will need.

What does a customer need to do next?

Informatica's customers should [log in to their account](#) and **submit a request via a support ticket to Informatica Global Customer Support** (GCS) to learn more about this offer for a temporary increase in licensed CPU-cores while evaluating these OS patches.

