Pure1™

The Meltdown and Spectre CPU Vulnerabilities

Pure Storage is aware of a reported potential security exposure with certain CPU components. These hardware vulnerabilities have been categorized into two attacks named the Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 and CVE-2017-5715) vulnerabilities 'Meltdown' and 'Spectre'.

From the available preliminary information that we have been provided to date, exploiting the vulnerability reportedly requires an attacker to run harmful code on the system itself and use that code to read kernel memory.

FlashBlade

On the Pure Storage FlashBlade product there is no mechanism to allow an administrator to add code or run untrusted code on the system so there is no known risk.

FlashArray

On the Pure Storage FlashArray product (not using the Purity Run feature) there is no mechanism to allow an administrator to add code or run untrusted code on the system so there is no known risk.

FlashArray with Purity Run

Pure is continuing to investigate the risk of any potential impact to FlashArrays using Purity Run. Purity Run allows customers to run applications provided by PureStorage on the FlashArray. Purity Run is a feature which can only be enabled with specific request from the customer to Pure Customer Support. Pure Customer Support will proactively reach out to every Pure customer using Purity Run. On FlashArrays with Purity Run enabled, the administrator should continue their usual practice of ensuring that only trusted code is executed in the Purity Run VM, and that access controls and patches are properly maintained.

Pure1

For Pure1 we are keeping our systems up to date with the latest security patches and are working with our vendors to ensure they are patching all their systems.

Additional Resources

Pure will continue to investigate as additional detail is provided by processor and OS providers.

https://newsroom.intel.com/news-releases/intel-issues-updates-protect-systems-security-exploits/

https://meltdownattack.com/

https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html