Data Security Notice: Meltdown and Spectre Remediation

Last Modified on 08/02/2022 12:57 pm EDT

In regards to the industry-wide processor in-memory security vulnerabilities known as “Meltdown” and “Spectre” **as of 1/12/2018** the PoliteMail data security administration team has completed their analysis and is confirming there is **no evidence of any use of these exploits** on any PoliteMail system.

CVE-2017-5715 branch target injection
CVE-2017-5353 bounds check bypass
CVE-2007-5754 rogue data cache load

Spectre Remediation Completed

For our **cloud services** customers, all Windows Server systems both our Microsoft Azure and Amazon AWS hosting providers have confirmed remediation of their infrastructures with all available patches applied against these vulnerabilities, and systems restarted.

We have surveyed all internal systems and equipment and all available patches have been applied as of 1/12/2018. Many vendors continue to work on these vulnerabilities and their variants and we will apply those patches as they become generally available.

Meltdown Remediation Plan In Progress

This has been classified as a low-risk vulnerability scenario for all production systems, as we do not execute untrusted code.

Systems vendors including Intel and Microsoft, have remediation updates and patches in progress to repair these vulnerabilities and their variants, and we will apply these as they become available.

Note that PoliteMail’s systems maintenance plans will automatically update all Windows Server and end-point security protection updates on the day they become available, these will be installed during the nightly maintenance window(s) and systems rebooted as necessary.