Meltdown and Spectre Detection and Remediation

Meltdown and Spectre Detection and Remediation

Two processor (CPU) flaws, called Meltdown and Spectre, have recently been publicly reported. These flaws could allow malicious code to read sensitive data such as passwords from protected areas of memory. This KB article will outline patch status from our vendors and review detection and remediation methods.

- **Sophos** – The required Sophos patch was released on January 9 and machines with Sophos installed have received this automatically. This patch created a required registry key that alerts Microsoft that it's safe to install the January security patches. The required registry setting and additional information can be found here:
  - https://community.sophos.com/kb/en-us/128060#Sophos.
- **Microsoft** -- The required January updates were approved in Windows Server Update Services (WSUS) on January 11. These will only install on machines with the correct registry setting mentioned above. Information Systems and Technology (IS&T) has confirmed that Sophos and built-in Windows antivirus software are working properly in this regard. If you are using other antivirus software, you will want to ensure the registry key exists. **Please note if this registry key is not applied, not only will you not get the January patches but you will no longer get any Windows patches.** Installing Windows updates will block only two out of three variants; a **firmware update is required for protection from the third variant.** More information is available here:
  - https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution
  - https://cloudblogs.microsoft.com/microsoftsecure/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-m
)
- **Firmware --** As mentioned above, firmware must be updated to an appropriate version or else you will not be fully protected. You can find specifics on firmware versions at these two links:
  - http://www.dell.com/support/article/us/en/04/sln308587/microprocessor-side-channel-vulnerabilities--cve-2017-5715--cve-2017-57
  - https://support.lenovo.com/us/en/solutions/LEN-18282
- **macOS** -- The only macOS protected against both Meltdown and Spectre is High Sierra 10.13.2 with the supplemental security patch and later. As of this writing, macOS 10.12 and 10.11 been patched for Meltdown (but not Spectre) with the 2018-001 security update, and have a patch available for Safari (see below). 10.10 and below should be upgraded to a newer OS. For more information, see:
  - https://support.apple.com/en-us/HT208397
  - https://support.apple.com/en-us/HT208465
- **Safari** -- Apple has released Safari 11.0.2 for macOS 10.11, 10.12, and 10.13. While it's important to install this new version of the browser, updating Safari does not remove the need to apply the macOS patches as they become available. For more information see:
  - https://support.apple.com/en-us/HT208403
- **iOS** -- Devices should be patched to 11.2.2. For more information, see:
  - https://support.apple.com/en-us/HT208401
- **Firefox** -- Firefox mainline has been patched and should be updated to 57.0.4 or later. Firefox ESR has been patched and should be updated to 52.6 or later. For more information, see:
  - https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack
- **Chrome** -- Chrome has been patched and should be updated to 64.0 or later. For more information, see:
  - https://support.google.com/faqs/answer/7622138#chrome

Remediation steps

The above vulnerabilities can be patched manually. The following KB articles have in depth information on automated remediation via Casper and SCCM.

- Casper
  - [Spectre / Meltdown detection via extension attribute]
  - Upgrade macOS to later version
  - Apply Apple software updates
  - Deploy software patches
  - Upgrade iOS to latest version
- SCCM
  - [Spectre / Meltdown detection via SCCM and PowerShell]
  - Detect Bios version
  - Automated 3rd party software patching (including Chrome and Firefox)
  - Software deployments
  - [Update the BIOS using SCCM]