**Spectre and Meltdown.**

To patch these vulnerabilities, windows needs patching and the BIOS updating.

Patching will address the following vulnerabilities:

* CVE-2017-5715 (branch target injection)
* CVE-2017-5753 (bounds check bypass)
* CVE-2017-5754 (rogue data cache load)

**Patch Windows**

**Part 1 Patch and set Regkeys**

Download all windows updates via control panel

Run script 1registrykeys.ps1

**Part 2 Check if patched**

To run the checks, you need to be using Windows Management Framework 5

Run script 2SpeculativeCheck.ps1

If This is already installed, accept the confirm boxes and let the test run.

Else wait for the download to appear in c:\temp

Then install Windows Management Framework 5 (will require reboot)

**Update BIOS**

**Part 3 get bios update**

Run script 3BiosDetails.ps1 compare the current BIOS version against the BIOS schedule.

<http://www.dell.com/support/article/us/en/04/sln308588/microprocessor-side-channel-vulnerabilities--cve-2017-5715--cve-2017-5753--cve-2017-5754---impact-on-dell-emc-products--dell-enterprise-servers--storage-and-networking-?lang=en>

Go to the manufacturers website to download and run a bios upgrade.

**Apply Changes**

**Part 4 Reboot Server**

**Part 5 Re-run script 2speculativeCheck.ps1 to confirm issue is resolved.**