MECM - SCCM - Verify Spectre - Meltdown Status on Windows

MECM - SCCM - Verify Spectre - Meltdown Status on Windows

Check Protection Status Using Queries

There are several queries in MECM to determine if your computers have received the OS patch from Microsoft to mitigate Spectre and Meltdown. There is a separate patch and associated KB number for each version of Windows. Please note that any machines in MECM are by default in the WIN domain which means they have already been opted into MIT's WSUS. This means they will automatically receive the necessary patches for Spectre/Meltdown.

If you check under Monitoring->Queries->MIT Queries you'll see the following:

- Missing Spectre/Meltdown Patch (Windows 10 v1607)
- Missing Spectre/Meltdown Patch (Windows 10 v1703)
- Missing Spectre/Meltdown Patch (Windows 10 v1709)
- Missing Spectre/Meltdown Patch (Windows 7 SP 1)

Each of these queries will list your computers than have not received the Spectre/Meltdown patch for the OS.

Check Protection Status Using PowerShell

You can check to see if your computers are protected against speculative execution side-channel vulnerabilities, aka Spectre and Meltdown, by using the follow PowerShell commands (right-click and run PowerShell prompt as an adminstrator):

```
PS > Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
PS > Install-Module SpeculationControl -Force
PS > Get-SpeculationControlSettings
```

This requires PowerShell 5.1 (included in Windows 10) or Windows Management Framework 5.1 if you are using older versions of PowerShell such as those included with Windows 7 or Windows 8.1.

The output of this PowerShell script will look like the following. Enabled protections will show in the output as “True”.

```
PS C:\> Get-SpeculationControlSettings
Speculation control settings for CVE-2017-5715 [branch target injection]

Hardware support for branch target injection mitigation is present: True

Windows OS support for branch target injection mitigation is present: True

Windows OS support for branch target injection mitigation is enabled: True

Speculation control settings for CVE-2017-5754 [rogue data cache load]

Hardware requires kernel VA shadowing: True

Windows OS support for kernel VA shadow is present: True

Windows OS support for kernel VA shadow is enabled: True

Windows OS support for PCID optimization is enabled: True
```

If you want to check the status via MECM, you can do so by running a PowerShell script via MECM. Right-click the device collection that you want to deploy the script to and select **Run Script**. Then choose the script **Check for Spectre and Meltdown**. Then click Next>, click Next>, and the click Close>.

Deploying the Spectre/Meltdown PowerShell Script on Windows 7
You'll need to first deploy the "EPM - Windows Management Framework 5.1 for Windows 7 (x64)" application from the MIT Applications folder if you do not already have this software installed on your client computers. Please note that this software requires a restart.

Check the output of the script by going to the Monitoring section of the MECM Console and looking under Script Status. You should see a script output for each computer in your collection. The output will be a long string of text and if you're seeing any "false" values, then you are not completely protected.

How to Remediate Vulnerabilities

Making sure your computers are protected is a combination of:

- Making sure your browsers are up-to-date - How to automate using Ninite Pro in MECM
- Getting Microsoft patches - Note that all domains computers will automatically receive Microsoft Patches from MIT's update server
- BIOS/firmware updates

See Also

- Microsoft Endpoint Configuration Manager (MECM) Landing Page