Meltdown and Spectre mitigation for organisations

By me

The website: *https://meltdownattack.com/*

Contents

Introduction

"Meltdown" is the following security vulnerabilities: CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

It needs code execution to function – if you are allowing untrusted parties to execute code, you may already have big security issues. If you are a cloud provider then the equation alters as you do not want one tenant to touch another.

Overview

CPU hardware implementations are vulnerable to side-channel attacks. These vulnerabilities are referred to as *Meltdown (https://meltdownattack.com/)* and *Spectre (https://spectreattack.com/)*.

Impact

An attacker able to execute code with user privileges can achieve various impacts, such as reading otherwise protected kernel memory and bypassing KASLR.

CVSS Metrics

Group	Score	Vector
Base	1.5	AV:L/AC:M/Au:S/C:P/I:N/A:N
Temporal	1.2	E:POC/RL:OF/RC:C
Environmental	2.0	CDP:ND/TD:H/CR:H/IR:ND/AR:ND

https://www.kb.cert.org/vuls/id/584653

Real world impact

This is an information disclosure vulnerability, for example retrieving data from memory. It is NOT a remote code execution vulnerability - you cannot use this to run malware. Microsoft's message: don't panic.

Windows Server and Client - antivirus

https://support.microsoft.com/en-us/help/4072699/important-information-regarding-the-windows-security-updates-released

"The compatibility issue is caused when anti-virus applications make unsupported calls into Windows kernel memory. These calls may cause stop errors (also known as blue screen errors) that make the device unable to boot. **To help prevent stop errors caused by incompatible anti-virus applications, Microsoft is only offering the Windows security updates released on January 3, 2018 to devices running anti-virus software from partners who have confirmed their software is compatible with the January 2018 Windows operating system security update**."

^^ you need to contact your AV provider and check their product is compatible, and make sure they add they registry key to say so. Otherwise you aren't getting protected.

Antivirus support chart – 4th January 2018

Vendor	Product	Sets registry key	Supported		Link

Microsoft	Windows Defender	Y	Y		
Kaspersky		Y	Y		*https://support.kaspersky.co.uk/14042*
ESET		Y	Y		
Sophos	Anti-Virus and Central	N	N	"Sophos plans to add registry key early next week"	*https://community.sophos.com/kb/en-us/128053*
Symantec	Endpoint Protection	Y	Y	Fix in Eraser Engine 117.3.0.359 - being pushed out	*https://pbs.twimg.com/media/DSsRaXBVoAEDpMR.jpg:larg*
Trend Micro		N	See link		*https://success.trendmicro.com/solution/1119183-importar updates*
Webroot		N	Y	Manual registry key setting - link to come	*https://community.webroot.com/t5/Security-Industry-News*
Cyren	F-PROT	N	N	Working on a fix, cannot set registry key thru usual update	
EMSI	Anti-Malware	N	N	Due later today or tomorrow	
McAfee	Endpoint Protection	N	N	"This is currently not supported - engineering team is working on it"	
Carbon Black		N	N	Assessing impact	
Cylance	PROTECT	N	N	Assessing impact	*https://pbs.twimg.com/media/DStLKBmW4AAmTKV.jpg:lar*
CrowdStrike	Falcon	N	Y	Requires manual registry key change currently	*https://pbs.twimg.com/media/DStIQkfWkAAPU49.jpg*

BitDefender		N	N	Fix this evening or tomorrow	*https://www.bitdefender.com/consumer/support/answ*
AVAST		Y	Y	Fix pushed yesterday to customers	*https://forum.avast.com/index.php?topic=212648.msg*
F-Secure	SAFE	Y	Y	Update out now. Legacy products tomorrow.	*https://community.f-secure.com/t5/F-Secure-SAFE/F-*

Windows Server

Microsoft guidance for Windows Server: *https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution-s*

Important note: **the patch is disabled by default** for performance reasons.

To enable the mitigations

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
```

Performance concerns with Windows Server

Microsoft say, having patched Azure, they have seen no CPU drop in performance. There are some huge numbers floating in the press for performance loss, however those were based on Linux testing – Microsoft say "question those numbers". You may not wish to enable the patch on all servers – for example, with heavily loaded Microsoft Exchange servers you shouldn't allow untrusted users to execute code, so therefore you may not want to take risk of a performance hit.

Windows Client

Microsoft guidance for Windows Client: *https://support.microsoft.com/en-us/help/4073119/windows-client-guidance-for-it-pros-to-protect-against-speculative-exe*

Mozilla Firefox

Firefox will be adding mitigations for websites trying to exploit in Firefox 57: *https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/5*

Google Chrome

Chrome 64, due late January, will include protection for websites trying to exploit: *https://www.chromium.org/Home/chromium-security/ssca*

Microsoft Edge and Internet Explorer 11

Microsoft have released an update yesterday which includes protection for websites trying to exploit: *https://blogs.windows.com/msedgedev/2018/01/03/speculative-execution-mitigations-microsoft-edge-internet-explorer/*

Amazon AWS - cloud

AWS has protected their customers: *https://aws.amazon.com/security/security-bulletins/AWS-2018-013/*

Azure

"The majority of Azure infrastructure has already been updated to address this vulnerability. Some aspects of Azure are still being updated and require a reboot of customer VMs for the security update to take effect. Many of you have received notification in recent weeks of a planned maintenance on Azure and have already rebooted your VMs to apply the fix, and no further action by you is required."
https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/

AMD processors

	Google Project Zero (GPZ) Research Title	**Details**
Variant One	Bounds Check Bypass	Resolved by software / OS updates to be made available by system vendors and manufacturers. Negligible performance impact expected.
Variant Two	Branch Target Injection	Differences in AMD architecture mean there is a near zero risk of exploitation of this variant. Vulnerability to Variant 2 has not been demonstrated on AMD processors to date.
Variant Three	Rogue Data Cache Load	Zero AMD vulnerability due to AMD architecture differences.

https://www.amd.com/en/corporate/speculative-execution
(https://www.amd.com/en/corporate/speculative-execution)

Xen hypervisors

You want to mitigate these ASAP, particularly if you use hypervisor as a security layer (e.g. bank or cloud provider): *https://xenbits.xen.org/xsa/advisory-254.html*

VMware

You want to patch these ASAP if you use hypervisor as a security layer (e.g. a bank or cloud provider). Advisory and patches: *https://blogs.vmware.com/security/2018/01/vmsa-2018-0002.html*

FAQ

I've read this can be exploited via a web browser.

Yes, there's a proof of concept via Javascript – however that is the Spectre vulnerability, not Meltdown. You can read memory in the PoC. Lots of security issues get fixed in browsers almost every month, including code execution (which is more serious) – so you just patch this like any other (browser makers have done or are doing a patch to prevent this PoC).