Meltdown and Spectre Mitigation

By Sathish Damodaran

Introduction

Meltdown allows attackers to read arbitrary physical memory (including kernel memory) for an unprivileged user process. Meltdown uses out of order instruction execution to leak data via a processor covert channel**.**

Spectre abuses branch prediction and speculative execution to leak data from via a processor covert channel. Spectre can only read memory from the current process, not the kernel or other physical memory

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

Meltdown - privilege escalation

On any unpatched system if any attacker can execute process they can dump all (or most) physical memory With physical memory, attackers could identify password hashes, execute a mimikartz style attack on windows or find private keys

Spectre – leaking browser memory

Using javascript (perhaps in an advertisement) spectre attacks could be used to leak browser cache or other saved data that pertains to other sites.

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

Solution and Workaround

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
Trend Micro		N	See link		https://success.trendmicro.com/solution/1119183-importantupdates
Webroot		N	Y	Manual registry key setting - link to come	
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
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	
AVAST		Y	Y	Fix pushed yesterday to customers	
F-Secure	SAFE	Y	Y	Update out now. Legacy products tomorrow.	

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

Linux Server

Kernel page table isolation (aka KPTI, aka the KAISER patch) removes the mapping of kernel memory in user space processes Because the kernel memory is no longer mapped, it cannot be read by meltdown. This incurs a non-negligible performance impact
https://lwn.net/Articles/738975/

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
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
As a workaround you can enable site isolation, this causes chrome to load each site into its own process so even if same origin policy is bypassed you can steal data from another site

Microsoft Edge and Internet Explorer 11

Microsoft have released an update on 3rd January 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/

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