Microsoft

January OOB Release

January 4, 2018

Henk van Roest CISSP
EMEA Security Program Manager
Twitter: @Henkvanroest

Overview

- New class of vulns - speculative execution side-channel attacks
  - Many CPU affected – Intel, AMD, ARM
  - Many OS- Windows, Linux, MacOS, iOS, Android
  - Impact= Information Disclosure
  - No active attacks detected
  - Won’t directly result in malware payload

What do I do?

1. Install Windows updates from 3rd January
2. Apply firmware update from OEM (CPU microcode)
3. Server OS need to enable software mitigations.

Windows client

- 1. Verify you are running a supported antivirus (AV) application before installing OS or firmware updates. Check with your antivirus software vendor for compatibility information.
- 2. Apply all available Windows operating system updates including the January 2018 Windows security updates.
- 3. Apply the applicable firmware update provided by your device manufacturer.
- More Info:

Windows Server

- 1. Apply all available Windows operating system updates including the January 2018 Windows security updates.
- 2. Apply the applicable firmware update provided by your device manufacturer.
- 3. Configure protections via registry

- More Info:

Cloud

- Public KB:

- Blog:

Official blog post:

Frequently Asked Questions

- Can my customer find out exactly when their VM will be rebooted? **No.**
- Has my customer been notified? **Yes**, an email and an in-portal service health notification s being sent to all impacted subscriptions.
- How long will the reboot take? We estimate completion with **30 minutes**.
- What if Service Health doesn't show a VM, or is blank? **No reboot needed**, this is being updated to "completed" or "already updated"
- Can a customer manually reboot now to avoid it? **Not guaranteed.**
- Does the guest OS need to be updated? **No**, not for this. But we always recommend that customers maintain the latest patch levels.
- Will there be a performance hit as a result of resolving this? In most circumstances, **no**. Accelerated networking is an option to consider.
- What about Azure PaaS services? All of these are **already** protected.
- How can my application know it's about to rebooted? Configure **scheduled events** to make an API call to the VM with 15 mins' notice.

Microsoft

Planned Maintenance **Field Q&A**

Azure

Official blog post:

- An industry-wide, hardware-based security vulnerability was disclosed today. Keeping customers secure is always our top priority and we are taking active steps to ensure that no Azure customer is exposed to these vulnerabilities. At the time of this blog post, Microsoft has not received any information to indicate that these vulnerabilities have been used to attack Azure customers.

- 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.

- With the public disclosure of the security vulnerability today, we are accelerating the planned maintenance timing and will begin automatically rebooting the remaining impacted VMs starting at 3:30pm PST on January 3, 2018. The self-service maintenance window that was available for some customers has now ended, in order to begin this accelerated update.

- During this update, we will maintain our SLA commitments of Availability Sets, VM Scale Sets, and Cloud Services. This reduces impact to availability and only reboots a subset of your VMs at any given time. This ensures that any solution that follows Azure's high availability guidance remains available to your customers and users. Operating system and Data disks on your VM will be retained during this maintenance. You can see the status of your VMs and if the reboot completed within the Azure Service Health Planned Maintenance Section in your Azure Portal.

- The majority of Azure customers should not see a noticeable performance impact with this update. We've worked to optimize the CPU and disk I/O path and are not seeing noticeable performance impact after the fix has been applied. A small set of customers may experience some networking performance impact. This can be addressed by turning on Azure Accelerated Networking (Windows, Linux), which is a free capability available to all Azure customers. We will continue to monitor performance closely and address customer feedback.

- This Azure infrastructure update addresses the disclosed vulnerability at the hypervisor level and does not require an update to your Windows or Linux VM images. However, as always, you should continue to apply security best practices for your VM images.

SQL

- Apply OS updates
- Specific SQL guidance should be live today

Additional Resources

Security Advisory 180002 - Vulnerability in CPU Microcode Could Allow Information Disclosure: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

KB 4073229 - Protect your device against the recent chip-related security vulnerability: https://support.microsoft.com/help/4073229

KB 4073119 - Windows Client Guidance for IT Pros to protect against the speculative execution side-channel vulnerabilities: https://support.microsoft.com/help/4073119

KB 4072698 - Windows Server Guidance to protect against the speculative execution side-channel vulnerabilities: https://support.microsoft.com/help/4072698

KB 4072699 - Important Information regarding the Windows Security Updates Released January 2018 (A/V): https://support.microsoft.com/help/4072699

KB 4073235 - Microsoft Cloud Protections Against Speculative Execution Side-Channel Vulnerabilities: https://support.microsoft.com/help/4073235

KB 4073065 - Surface Guidance for Customers and Partners “Protect your devices against the recent chip-related security vulnerability”: https://support.microsoft.com/help/4073065