Processor Speculative Execution Research Disclosure

Concerning: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update As Of: 2018/02/05 4:30 PM PST

This is an update for this issue.

An updated kernel for Amazon Linux is available within the Amazon Linux repositories. EC2 instances launched with the default Amazon Linux configuration on or after January 13th, 2018 will automatically include the updated package, which incorporates the latest stable open source Linux security improvements to address CVE-2017-5715 within the kernel and builds upon previously incorporated Kernel Page Table Isolation (KPTI) that addressed CVE-2017-5754. Customers must upgrade to the latest Amazon Linux kernel or AMI to effectively mitigate process-to-process concerns of CVE-2017-5715 and process-to-kernel concerns of CVE-2017-5754 within their instances. See "Processor Speculative Execution – Operating System Updates" for more information.

Please see "PV Instance Guidance" information further below concerning para-virtualized (PV) instances.

Amazon EC2

All instances across the Amazon EC2 fleet are protected from all known instance-to-instance concerns of CVE-2017-5715, CVE-2017-5753, and CVE-2017-5754. Instance-to-instance concerns assume an untrusted neighbor instance could read the memory of another instance or the AWS hypervisor. This issue has been addressed for AWS hypervisors, and no instance can read the memory of another instance, nor can any instance read AWS hypervisor memory. As previously stated, we have not observed meaningful performance impact for the overwhelming majority of EC2 workloads.

As of January 12, 2018, we finished de-activating portions of the new Intel CPU microcode for the platforms in AWS where we were seeing a small number of crashes and other unpredictable behavior caused by the Intel microcode updates. This change mitigated these issues for this small

~~Amazon Elastic Container Service, Amazon Elastic MapReduce, and Amazon Lightsail~~

While all customer instances are protected as described above, we recommend that customers patch their instance operating systems to address process-to-process or process-to-kernel concerns of this issue. Please see "Processor Speculative Execution – Operating System Updates" for further guidance and instructions for Amazon Linux & Amazon Linux 2, CentOS, Debian, Fedora, Microsoft Windows, Red Hat, SUSE, and Ubuntu.

PV Instance Guidance

After ongoing research and detailed analysis of operating system patches available for this issue, we have determined that operating system protections are insufficient to address process-to-process concerns within para-virtualized (PV) instances. While PV instances are protected by AWS hypervisors from any instance-to-instance concerns as described above, customers concerned with process isolation within their PV instances (eg. process untrusted data, run untrusted code, host untrusted users), are strongly encouraged to migrate to HVM instance types for longer-term security benefits.

For more information on the differences between PV and HVM (as well as instance upgrade path documentation), please see:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/virtualization_types.html

Please engage Support if you require assistance with an upgrade path for any PV instances.

Updates to other AWS services

The following services required patching of EC2 instances managed on behalf of customers, have completed all work, and no customer action is required:

- Fargate
- Lambda

Unless otherwise discussed below, all other AWS services do not require customer action.

ECS Optimized AMI

We have released Amazon ECS Optimized AMI version 2017.09.g which incorporates all Amazon Linux protections for this issue. We advise all Amazon ECS customers to upgrade to this latest version which is available in the AWS Marketplace.

Customers that choose to update existing ECS Optimized AMI instances in place should run the following command to ensure they receive the updated package:

```
sudo yum update kernel
```

Linux customers who do not use the ECS Optimized AMI are advised to consult with the vendor of any alternative / third-party operating system, software, or AMI for updates and instructions as needed. Instructions about Amazon Linux are available in the Amazon Linux AMI Security Center.

We have released Amazon ECS Optimized Windows AMI version 2018.01.10. For details about how to apply patches to running instances, see "Processor Speculative Execution – Operating System Updates".

Elastic Beanstalk

We have updated all Linux-based platforms to include all Amazon Linux protections for this issue. See the release notes for specific platform versions. We advise Elastic Beanstalk customers to update their environments to the latest available platform version. Environments using Managed Updates will be automatically updated during the configured maintenance window.

Windows-based platforms have also been updated to include all EC2 Windows protections for this issue. Customers are advised to update their Windows-based Elastic Beanstalk environments to the latest available platform configuration.

ElastiCache

ElastiCache-managed customer cache nodes are each dedicated to only running a cache engine for a single customer, with no other customer-accessible processes and no ability for customers to run code on the underlying instance. As AWS has finished protecting all infrastructure underlying ElastiCache, process-to-kernel or process-to-process concerns of this issue do not present a risk to customers. Both cache engines ElastiCache supports have reported no known intra-process concerns at this time.

EMR

Amazon EMR launches clusters of Amazon EC2 instances running Amazon Linux on behalf of customers into the customer's account. Customers concerned with process isolation within the instances of their Amazon EMR clusters should upgrade to the latest Amazon Linux kernel as recommended above. We have incorporated the latest Amazon Linux kernel into new minor releases 5.11.1, 5.8.1, 5.5.1, and 4.9.3. Customers can create new Amazon EMR clusters with these releases.

For current Amazon EMR releases and any associated running instances customers may have, we recommend updating to the latest Amazon Linux kernel as recommended above. For new clusters, customers can use a bootstrap action to update the Linux kernel and reboot each instance. For running clusters, customers can facilitate the Linux kernel update and restart for each instance in their cluster in a rolling fashion. Please note that restarting certain processes can impact running applications within the cluster.

RDS

RDS, process-to-kernel or process-to-process concerns of this issue do not present a risk to customers. Most database engines RDS supports have reported no known intra-process concerns at this time. Additional database engine-specific details are below, and unless otherwise noted, there is no customer action required.

For RDS for SQL Server Database Instances, we will release OS and database engine patches as Microsoft makes each available, allowing customers to upgrade at a time of their choosing. We will update this bulletin when either has been completed. In the meantime, customers who have enabled CLR (disabled by default) should review Microsoft's guidance on disabling the CLR extension at https://support.microsoft.com/en-us/help/4073225/guidance-for-sql-server.

For RDS PostgreSQL and Aurora PostgreSQL, DB Instances running in the default configuration currently have no customer actions required. We will provide the appropriate patches for users of plv8 extensions once they are made available. In the meantime, customers who have enabled plv8 extensions (disabled by default) should consider disabling them and review V8's guidance at https://github.com/v8/v8/wiki/Untrusted-code-mitigations.

RDS for MariaDB, RDS for MySQL, Aurora MySQL, and RDS for Oracle database instances currently have no customer actions required.

VMware Cloud on AWS

Per VMware, “The remediation as documented in VMSA-2018-0002, has been present in VMware Cloud on AWS since early December 2017.”

Please refer to the VMware Security & Compliance Blog for more details and https://status.vmware-services.io for updated status.

WorkSpaces

For Windows 7 experience on Windows Server 2008 R2 customers:

Microsoft has released new security updates for Windows Server 2008 R2 for this issue. Successful delivery of these updates requires compatible Antivirus software running on the server as outlined in the security update by Microsoft: https://support.microsoft.com/en-us/help/4072699/january-3-2018-windows-security-updates-and-antivirus-software. WorkSpaces customers need to take action to get these updates. Please follow the instructions provided by Microsoft at: https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution.

For Windows 10 experience on Windows Server 2016 customers:

AWS has applied security updates to WorkSpaces running the Windows 10 experience on Windows Server 2016. Windows 10 has built in Windows Defender AntiVirus software which is compatible with these security updates. No further customer action is required.

customers who have changed the default update settings in their WorkSpaces should manually apply the security updates provided by Microsoft. If this applies to you, please follow the instructions provided by the Microsoft security advisory at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002. The security advisory includes links to knowledge base articles for both Windows Server and Client operating systems that provide further specific information.

Updated WorkSpaces bundles will be available with the security updates soon. Customers who have created Custom Bundles should update their bundles to include the security updates themselves. Any new WorkSpaces launched from bundles that do not have the updates will receive patches soon after launch, unless customers have changed the default update setting in their WorkSpaces or installed incompatible antivirus software, in which case they should follow the above steps to manually apply the security updates provided by Microsoft.

WorkSpaces Application Manager (WAM)

We recommend that customers choose one of the following courses of action:

Option 1: Manually apply the Microsoft updates on running instances of WAM Packager and Validator by following the steps provided by Microsoft at https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution . This page provides further instructions and relevant downloads.

Option 2: Terminate your existing Packager and Validator instances. Launch new instances using our updated AMIs labeled "Amazon WAM Admin Studio 1.5.1" and "Amazon WAM Admin Player 1.5.1".

SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Test Drives
AWS Business Builder

Manage Your Account
Management Console
Billing & Cost Management
Subscribe to Updates
Personal Information
Payment Method
AWS Identity & Access Management
Security Credentials
Request Service Limit Increases
Contact Us