Mirantis Technical Bulletin 2019-009

December 11, 2019

TSX Asynchronous Abort vulnerability in Intel processors, Intel® processor machine check error vulnerability, and i915 graphic driver flaws

ISSUE

The number of vulnerabilities affecting Intel processors has been recently disclosed. This includes:

- CVE-2019-11135 [0] TSX Asynchronous Abort (TAA) vulnerability in Intel processors
- CVE-2018-12207 [1] Intel® Processor Machine Check Error on Page Size Change (MCEPSC) Speculative-Execution vulnerability
- CVE-2019-0155 [2] and CVE-2019-0154 [3] i915 Graphic Driver Flaws

To mitigate these issues, you should update your processor microcode and Linux kernel to certain versions. For more details, see the TAA_MCEPSC_i91 [4] article in the Ubuntu knowledge base.

Additionally to the fixes of the vulnerabilities mentioned above, the kernel and `intel-microcode` package versions proposed in this technical bulletin also contain fixes for:

- CVE-2019-14835 [5]
- USN-4182-3 [6]

AFFECTS

The affected MCP versions include MCP 2019.2.6 maintenance update and earlier.

If your cluster runs on top of MCP 2019.2.6 or earlier 2019.2.x maintenance update, apply the MCP 2019.2.7 maintenance update when it is available. Otherwise, proceed with the steps in this bulletin.

This technical bulletin is intended for customers running MCP 2018.4, 2018.8, and 2018.11 versions with Ubuntu 16.04.

SECURITY IMPACT

High

ESTIMATED TIME REQUIRED TO APPLY THE FIX

The time calculations are based on the size of the default MCP deployment and do not take into account the time required for preparation steps.

> **CAUTION:** A maintenance window should be planned carefully and may differ on the size of the cluster. Please, refer to MCP Operations Guide > Scheduled maintenance with a planned power outage [7] to properly plan the maintenance window.

The time estimation for the update operations:

- Copying files to nodes and installing the software require approximately 15 minutes depending on the size of the environment and the `-b 1` option used while installing the packages.
- Restarting the nodes after update requires 7-15 minutes depending on the role of the node.
- Verifying the update requires approximately 30 minutes.

HOW TO DETERMINE IF YOU ARE AFFECTED

1. Log in to the Salt Master node and start the `screen` session:

   ```
   screen
   ```

2. For all nodes, verify the versions of the kernel and `intel-microcode` package:

   ```
   sudo salt '*' cmd.run 'uname -srv'
   sudo salt '*' pkg.version intel-microcode
   ```

   If the version of the kernel is below `4.15.0-70.79~16.04.1` and the version of the `intel-microcode` package is below `3.20191112-0ubuntu0.16.04.2`, the cluster is affected.

STEPS TO CORRECT

The fix is applicable only to the clusters that are running MCP 2018.4, 2018.8, and 2018.11 versions with Ubuntu 16.04. Perform the following steps on the Salt Master node unless another node is explicitly specified.

To apply the update:

1. Log in to the Salt Master node and start the `screen` session:

```
screen
```

2. Download the `34039-taa_mcepsc_i915-xenial.tar.gz` archive from Artifactory [8]:

```
wget
https://artifactory.mirantis.com/artifactory/fixes/34039-taa_mcepsc_i915
-xenial.tar.gz
```

3. Unpack the archive:

```
tar -xvzf 34039-taa_mcepsc_i915-xenial.tar.gz
cd 34039-taa_mcepsc_i915-xenial
```

4. Copy the required `.deb` packages to the target nodes.
   The unpacked archive contains packages for the base kernel (folder `4.4.0-169.198`) and for the enablement (HWE) kernel (folder `4.15.0-70.79~16.04.1`). Determine which kernel is used on your system and change the directory to the necessary folder.

   CAUTION: Your environment may contain nodes with both types of kernels. Verify that you copy the files to the proper directory before proceeding.

   For example:

```
cd 4.4.0-169.198
```

5. Copy the required `.deb` packages to the target nodes:

   CAUTION: When using the `scp` command, verify that the destination folder has correct permissions for the SSH user.

```
sudo salt "*" cmd.run "mkdir -p /tmp/kernel_pkgs/"

sudo salt "*" cmd.run "chown <your_ssh_user> /tmp/kernel_pkgs/"

for i in $(sudo salt "*" test.ping --out=txt|cut -d':' -f1); do scp -o
"StrictHostKeyChecking no" *.deb $i:/tmp/kernel_pkgs/; done
```

If your environment has OpenContrail deployed, you should additionally copy the `linux-headers` package to the CMP nodes:

```
for i in $(sudo salt "cmp*" test.ping --out=txt|cut -d':' -f1); do scp
-o "StrictHostKeyChecking no" headers/*.deb $i:/tmp/kernel_pkgs/; done
```

6. Verify that the required `.deb` packages exist on the target nodes:

```
sudo salt "*" cmd.run "ls -l /tmp/kernel_pkgs/"
```

7. Create a backup list of the installed packages:

```
sudo salt '*' cmd.run 'uname -srv' >> ~/old_kernel_version.txt
```

8. Update the packages on the Salt Master node:

```
sudo salt 'cfg*' -b 1 cmd.run 'export DEBIAN_FRONTEND=noninteractive;
apt-get install -yq -f /tmp/kernel_pkgs/*'
```

9. Restart the Salt Master node:

```
sudo salt 'cfg*' -b 1 --batch-wait 150 --timeout=1 system.reboot
```

10. Update the packages on the rest of nodes:

CAUTION: The command below starts the update process on all nodes except the Salt Master node one by one with the 2-minute timeout. If you want to update nodes in a different order, change the compound matcher.

```
sudo salt -C '* and not cfg*' -b 1 --batch-wait 120 cmd.run 'export
DEBIAN_FRONTEND=noninteractive; apt-get install -yq -f
/tmp/kernel_pkgs/*'
```

11. Restart the nodes.

    After applying the kernel and `intel-microcode` updates, you must schedule a restart of all MCP nodes. Plan a maintenance window for the reboot based on MCP Operations Guide > Scheduled maintenance with a planned power outage [7].

12. Verify that the packages have been updated and check the system status:

```
sudo salt '*' cmd.run 'uname -srv'
sudo salt '*' pkg.version intel-microcode
sudo salt '*' cmd.run "dpkg -l |grep linux |grep -E '4.15|4.4'"
```

    The packages versions should match or be higher than the versions of the packages located in the archive.

    4.15.0-70.79~16.04.1 packages in the archive:

    - `headers/linux-headers-4.15.0-70_4.15.0-70.79~16.04.1_all.deb`
    - `headers/linux-headers-4.15.0-70-generic_4.15.0-70.79~16.04.1_amd64.deb`
    - `intel-microcode_3.20191115.1ubuntu0.16.04.2_amd64.deb`
    - `linux-base_4.5ubuntu1~16.04.1_all.deb`
    - `linux-image-4.15.0-70-generic_4.15.0-70.79~16.04.1_amd64.deb`
    - `linux-image-extra-virtual-hwe-16.04_4.15.0.70.90_amd64.deb`
    - `linux-image-generic-hwe-16.04_4.15.0.70.90_amd64.deb`
    - `linux-image-virtual-hwe-16.04_4.15.0.70.90_amd64.deb`
    - `linux-modules-4.15.0-70-generic_4.15.0-70.79~16.04.1_amd64.deb`
    - `linux-modules-extra-4.15.0-70-generic_4.15.0-70.79~16.04.1_amd64.deb`

    4.4.0-169.198 packages in the archive:

    - `headers/linux-headers-4.4.0-169_4.4.0-169.198_all.deb`
    - `headers/linux-headers-4.4.0-169-generic_4.4.0-169.198_amd64.deb`
    - `intel-microcode_3.20191115.1ubuntu0.16.04.2_amd64.deb`
    - `linux-base_4.5ubuntu1~16.04.1_all.deb`
    - `linux-image-4.4.0-169-generic_4.4.0-169.198_amd64.deb`
    - `linux-image-extra-virtual_4.4.0.169.177_amd64.deb`
    - `linux-image-generic_4.4.0.169.177_amd64.deb`
    - `linux-image-virtual_4.4.0.169.177_amd64.deb`
    - `linux-modules-4.4.0-169-generic_4.4.0-169.198_amd64.deb`
    - `linux-modules-extra-4.4.0-169-generic_4.4.0-169.198_amd64.deb`

    If all packages have been updated correctly, proceed with the system status verification as described in TAA_MCEPSC_i915 > Checking System Status section [4] in the Ubuntu knowledge base.

STEPS TO REVERT THE PATCH

To revert the patch, start the system from the previous version of the kernel:

1. Log in to the target node.
2. Verify that the previously installed kernel version is available in the system:

```
ls /boot |grep vmlinuz
```

Example of system response:

```
vmlinuz-4.4.0-128-generic
vmlinuz-4.4.0-169-generic
```

3. Verify that the menu entry for the previously installed kernel version exists in `grub.cfg`:

```
awk -F\' '/menuentry / {print $2}' /boot/grub/grub.cfg
```

Example of system response:

```
Ubuntu
Ubuntu, with Linux 4.4.0-169-generic
Ubuntu, with Linux 4.4.0-169-generic (recovery mode)
Ubuntu, with Linux 4.4.0-128-generic
Ubuntu, with Linux 4.4.0-128-generic (recovery mode)
```

CAUTION: From this response, you can decide which value you should use for the `GRUB_DEFAULT` option:

- **`GRUB_DEFAULT=0`** Ubuntu
- **`GRUB_DEFAULT="1>0"`** Ubuntu, with Linux 4.4.0-169-generic
- **`GRUB_DEFAULT="1>1"`** Ubuntu, with Linux 4.4.0-169-generic (recovery mode)
- **`GRUB_DEFAULT="1>2"`** Ubuntu, with Linux 4.4.0-128-generic
- **`GRUB_DEFAULT="1>3"`** Ubuntu, with Linux 4.4.0-128-generic (recovery mode)

4. Open the `grub` configuration file in `/etc/default/grub` and edit the `GRUB_DEFAULT` option to select the previously installed kernel version:

Example of the `/etc/default/grub` file before editing:

```
GRUB_DEFAULT=0
```

```
GRUB_HIDDEN_TIMEOUT=0
GRUB_HIDDEN_TIMEOUT_QUIET=true
GRUB_TIMEOUT=0
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8"
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8"
```

Example of the `/etc/default/grub` file after editing:

```
#GRUB_DEFAULT=0
GRUB_DEFAULT="1>2"
GRUB_HIDDEN_TIMEOUT=0
GRUB_HIDDEN_TIMEOUT_QUIET=true
GRUB_TIMEOUT=0
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8"
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8"
```

5. Update `grub` and reboot the system:

```
sudo update-grub
sudo reboot
```

REFERENCES

[0] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11135

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12207

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0155

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0154

[4] https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/TAA_MCEPSC_i915

[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14835

[6] https://usn.ubuntu.com/4182-3/

[7] https://docs.mirantis.com/mcp/q4-18/mcp-operations-guide/scheduled-maintenance-power-outage.html

[8] https://artifactory.mcp.mirantis.net/artifactory/fixes/34039-taa_mcepsc_i915-xenial.tar.gz