

VMWare ESXi

- Unzulässigen Hostnamen ändern
- CVE-2018-3646
- SNMP Aktivieren

Unzulässigen Hostnamen ändern

Per SSH Verbinden und:

```
esxcfg-advcfg -s ESXi_4 /Misc/hostname
```

Wo ESXi_4 der Hostname des Servers sein soll, anfangs sollte das system "localhost.localdomain" sagen, das wird damit geändert so heißt das Ding nachher nur noch "ESXi_4"

CVE-2018-3646

Dieser Host ist potenziell anfällig für in CVE-2018-3646 beschriebene Probleme; Details und VMware-Empfehlungen finden Sie in <https://kb.vmware.com/s/article/55636>.

 Dieser Host ist potenziell anfällig für in CVE-2018-3646 beschriebene Probleme; Details und VMware-Empfehlungen finden Sie in <https://kb.vmware.com/s/article/55636>. 

SSH:

```
esxcli system settings kernel set -s hyperthreadingMitigation -v TRUE
```

Quelle: <https://knowledge.broadcom.com/external/article?legacyId=55806>

1. Update Phase: Apply vSphere Updates and Patches

The Sequential-context attack vector is mitigated by a vSphere update to the product versions listed in VMware Security Advisory VMSA-2018-0020. This mitigation is dependent on Intel microcode updates (provided in separate ESXi patches for most Intel hardware platforms) which are also documented in VMSA-2018-0020. This mitigation is enabled by default and does not impose a significant performance impact.

Note: As displayed in the workflow above, vCenter Server should be updated prior to applying ESXi patches. Notification messages were added in the aforementioned updates and patches to explain that the ESXi Side-Channel-Aware Scheduler must be enabled to mitigate the Concurrent-context attack vector of CVE-2018-3646. If ESXi is updated prior to vCenter you may receive cryptic notification messages relating to this. After vCenter has been updated, the notifications will be shown correctly.

2. Planning Phase: Assess Your Environment

The Concurrent-context attack vector is mitigated through enablement of the ESXi Side-Channel-Aware Scheduler which is included in the updates and patches listed in VMSA-2018-0020. This scheduler is not enabled by default. Enablement of this scheduler may impose a non-trivial performance impact on applications running in a vSphere environment. The goal of the Planning Phase is to understand if your current environment has sufficient CPU capacity to enable the scheduler without operational impact.

The following list summarizes potential problem areas after enabling the ESXi Side-Channel-

Aware Scheduler:

- VMs configured with vCPUs greater than the physical cores available on the ESXi host
- VMs configured with custom affinity or NUMA settings
- VMs with latency-sensitive configuration
- ESXi hosts with Average CPU Usage greater than 70%
- Hosts with custom CPU resource management options enabled
- HA Clusters where a rolling upgrade will increase Average CPU Usage above 100%

Important: The above list is meant to be a brief overview of potential problem areas related to enablement of the ESXi Side-Channel-Aware Scheduler.

Note: It may be necessary to acquire additional hardware, or rebalance existing workloads, before enablement of the ESXi Side-Channel-Aware Scheduler. Organizations can choose not to enable the ESXi Side-Channel-Aware Scheduler after performing a risk assessment and accepting the risk posed by the Concurrent-context attack vector. This is NOT RECOMMENDED and VMware cannot make this decision on behalf of an organization.

3. **Scheduler-Enablement Phase:**

- a. **Enable the ESXi Side-Channel-Aware Scheduler in ESXi 5.5, 6.0, 6.5, and 6.7 (prior to 6.7u2) and 7.0.**

After addressing the potential problem areas described above during the Planning Phase, the ESXi Side-Channel-Aware Scheduler must be enabled to mitigate the Concurrent-context attack vector of CVE-2018-3646. The scheduler can be enabled on an individual ESXi host via the advanced configuration option *hyperthreadingMitigation*.

Notes:

- Enabling this option will result in the vSphere UI reporting only a single logical processor per physical core; halving the number of logical processors if Hyperthreading was previously enabled. In addition Hyperthreading may be reported as 'Disabled' in various configuration tabs.
- The current ESXi Side-Channel-Aware scheduler also addresses CVE-2018-5407.

Enabling the ESXi Side-Channel-Aware Scheduler using the vSphere Web Client or vSphere Client

1. Connect to the vCenter Server using either the vSphere Web or vSphere Client.
2. Select an ESXi host in the inventory.
3. Click the **Manage** (5.5/6.0) or Configure (6.5/6.7/7.0) tab.
4. Click the **Settings** sub-tab.
5. Under the System heading, click **Advanced System Settings**.

6. Click in the Filter box and search
`VMkernel.Boot.hyperthreadingMitigation`
7. Select the setting by name and click the **Edit** pencil icon.
8. Change the configuration option to true (default: false).
9. Click **OK**.
10. Reboot the ESXi host for the configuration change to go into effect.

Enabling the ESXi Side-Channel-Aware Scheduler using ESXi Embedded Host Client

1. Connect to the ESXi host by opening a web browser to `https://HOSTNAME`.
2. Click the **Manage** tab.
3. Click the **Advanced settings** sub-tab.
4. Click in the Filter box and search
`VMkernel.Boot.hyperthreadingMitigation`
5. Select the setting by name and click the **Edit** pencil icon.
6. Change the configuration option to true (default: false).
7. Click **Save**.
8. Reboot the ESXi host for the configuration change to go into effect.

Enable ESXi Side-Channel-Aware Scheduler setting using ESXCLI

1. SSH to an ESXi host or open a console where the remote ESXCLI is installed. For more information, see the ESXCLI Developer Portal.
2. Check the current runtime value of the HTAware Mitigation Setting by running `esxcli system settings kernel list -o hyperthreadingMitigation`
3. To enable HT Aware Mitigation, run this command:

```
esxcli system settings kernel set -s hyperthreadingMitigation -v TRUE
```

4. Reboot the ESXi host for the configuration change to go into effect.

b. Enable the ESXi Side-Channel-Aware Scheduler (SCAv1) or the ESXi Side-Channel-Aware Scheduler v2 (SCAv2) in ESXi 6.7u2 (13006603) or later

Note: ESXi 6.7u2 (13006603) and future release lines of ESXi include the ESXi Side-Channel-Aware Scheduler v2. Prior release lines such as 6.5, 6.0, and 5.5 cannot accommodate this new scheduler.



VMware has published a white paper entitled Performance of vSphere 6.7 Scheduling Options which provides a more detailed look into the performance differences between SCAv1 and SCAv2. Please review this document before continuing.

Enabling the ESXi Side-Channel-Aware Scheduler (SCAv1) using the vSphere Web Client or vSphere Client

1. Connect to the vCenter Server using either the vSphere Web or vSphere Client.
2. Select an ESXi host in the inventory.
3. Click the Configure tab.
4. Under the System heading, click **Advanced System Settings**.
5. Click **Edit**.
6. Click in the Filter box and search VMkernel.Boot.hyperthreadingMitigation.
7. Select the setting by name.
8. Change the configuration option to true (default: false).
9. Click in the Filter box and search VMkernel.Boot.hyperthreadingMitigationIntraVM.
10. Change the configuration option to true (default: true).
11. Click **OK**.
12. Reboot the ESXi host for the configuration change to go into effect.

Enabling the ESXi Side-Channel-Aware Scheduler (SCAv1) using ESXi Embedded Host Client

1. Connect to the ESXi host by opening a web browser to <https://HOSTNAME>.
2. Click **Manage** under host navigator.
3. Click the **Advanced settings** Tab.
4. Use the search box to find VMkernel.Boot.hyperthreadingMitigation
5. Select the VMkernel.Boot.hyperthreadingMitigation setting and click the **Edit** Option.
6. Change the configuration option to true (default: false).
7. Click **Save**.
8. Use the search box to find VMkernel.Boot.hyperthreadingMitigationIntraVM.
9. Select the VMkernel.Boot.hyperthreadingMitigationIntraVM setting and click the **Edit** Option.
10. Change the configuration option to true (default: true).
11. Click **Save**.
12. Reboot the ESXi host for the configuration change to go into effect.

Enable ESXi Side-Channel-Aware Scheduler (SCAv1) using ESXCLI

1. SSH to an ESXi host or open a console where the remote ESXCLI is installed. For more information, see the [ESXCLI Developer Portal](#).
2. Check the current runtime values by running `esxcli system settings kernel list -o hyperthreadingMitigation` and `esxcli system settings kernel list -o hyperthreadingMitigationIntraVM`.
3. To enable the ESXi Side-Channel-Aware Scheduler Version 1 run these commands:
4. `esxcli system settings kernel set -s hyperthreadingMitigation -v TRUE`
5. `esxcli system settings kernel set -s hyperthreadingMitigationIntraVM -v TRUE`
6. Reboot the ESXi host for the configuration change to go into effect.

Enabling the ESXi Side-Channel-Aware Scheduler Version 2 (SCAv2) using the vSphere Web Client or vSphere Client

1. Connect to the vCenter Server using either the vSphere Web or vSphere Client.
2. Select an ESXi host in the inventory.
3. Click the Configure tab.

4. Under the System heading, click **Advanced System Settings**.
5. Click **Edit**.
6. Click in the Filter box and search VMkernel.Boot.hyperthreadingMitigation.
7. Select the setting by name.
8. Change the configuration option to true (default: false).
9. Click in the Filter box and search VMkernel.Boot.hyperthreadingMitigationIntraVM.
10. Change the configuration option to false (default: true).
11. Click **OK**.
12. Reboot the ESXi host for the configuration change to go into effect.

Enabling the ESXi Side-Channel-Aware Scheduler Version 2 (SCAv2) using ESXi Embedded Host Client

1. Connect to the ESXi host by opening a web browser to <https://HOSTNAME>.
2. Click **Manage** under host navigator.
3. Click the **Advanced settings** Tab.
4. Use the search box to find VMkernel.Boot.hyperthreadingMitigation.
5. Select the VMkernel.Boot.hyperthreadingMitigation setting and click the **Edit** Option.
6. Change the configuration option to true (default: false).
7. Click **Save**.
8. Use the search box to find VMkernel.Boot.hyperthreadingMitigationIntraVM.
9. Select the VMkernel.Boot.hyperthreadingMitigationIntraVM setting and click the **Edit** Option.
10. Change the configuration option to false (default: true).
11. Click **Save**.
12. Reboot the ESXi host for the configuration change to go into effect.

Enable ESXi Side-Channel-Aware Scheduler Version 2 (SCAv2) using ESXCLI

1. SSH to an ESXi host or open a console where the remote ESXCLI is installed. For more information, see the [ESXCLI Developer Portal](#).
2. Check the current runtime values by running `esxcli system settings kernel list -o hyperthreadingMitigation` and `esxcli system settings kernel list -o hyperthreadingMitigationIntraVM`
3. To enable the ESXi Side-Channel-Aware Scheduler Version 1 run these commands:
4. `esxcli system settings kernel set -s hyperthreadingMitigation -v TRUE`
5. `esxcli system settings kernel set -s hyperthreadingMitigationIntraVM -v FALSE`
6. Reboot the ESXi host for the configuration change to go into effect.

ESXi 6.7u2 (and later) Scheduler Configuration Summary

hyperthreadingMitigation	hyperthreadingMitigationIntraVM	Scheduler Enabled
FALSE	TRUE or FALSE	Default scheduler (unmitigated)
TRUE	TRUE	SCAv1
TRUE	FALSE	SCAv2

HTAware Mitigation Tool

VMware has provided a tool to assist in performing both the **Planning Phase** and the **Scheduler-Enablement Phase** at scale. This tool has been updated to include SCAv2 support and can be found in [HTAware Mitigation Tool Overview and Usage \(328935\)](#) along with detailed instructions on its usage, capabilities, and limitations.

Table 1: Affected Intel Processors Supported by ESXi

Intel Code Name	FMS	Intel Brand Names
Nehalem-EP	0x106a5	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Lynnfield	0x106e5	Intel Xeon 34xx Lynnfield Series
Clarkdale	0x20652	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d7	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9	Intel i3-3200 Series; Intel i7-3500-LE/UE, Intel i7-3600-QE, Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C
Haswell DT	0x306c3	Intel Xeon E3-1200-v3 Series
Ivy Bridge EP	0x306e4	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-1400-v2 Series; Intel Xeon E5-2600-v2 Series
Ivy Bridge EX	0x306e7	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2	Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-4600-v3 Series
Haswell EX	0x306f4	Intel Xeon E7-8800/4800-v3 Series

Broadwell H	0x40671	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series
Skylake SP	0x50654	Intel Xeon Platinum 8100 (Skylake-SP) Series; Intel Xeon Gold 6100/5100 (Skylake-SP) Series Intel Xeon Silver 4100, Bronze 3100 (Skylake-SP) Series
Broadwell DE	0x50662	Intel Xeon D-1500 Series
Broadwell DE	0x50663	Intel Xeon D-1500 Series
Broadwell DE	0x50664	Intel Xeon D-1500 Series
Broadwell NS	0x50665	Intel Xeon D-1500 Series
Skylake H/S	0x506e3	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Kaby Lake H/S/X	0x906e9	Intel Xeon E3-1200-v6

SNMP Aktivieren

In arbeit

SSH

```
[root@ESXi_3:~] esxcli system snmp set --enable true
[root@ESXi_3:~] esxcli system snmp set --authentication SHA1
[root@ESXi_3:~] esxcli system snmp set --privacy AES128
[root@ESXi_3:~] esxcli system snmp hash --priv-hash --raw-secret -A
Enter value for 'priv-hash':
Enter value for 'auth-hash':
Authhash: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Privhash: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
[root@ESXi_3:~] esxcli system snmp set --users
max/FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/priv
```