Initial Publication: 1/18/18 7:47:00 AM
Last Update: 1/3/2019 9:25:00 AM

SUMMARY:

The side-channel security vulnerabilities commonly known as Meltdown and Spectre affect the SPHiNX virtual tapes appliance server.

This document provides a work of statement for mitigating the security vulnerabilities on SPHiNX appliance server and branded OEM Virtual TapeServer[1].

DISCLAIMER:

ETI\SPHINX INC. ("ETI-SPHiNX") is distributing this communication in an effort to bring to users' attention important information on the potentially affected servers running SPHiNX appliance. ETI-SPHiNX recommends to use the information as specified, based on each user's configuration, and to take appropriate action. ETI-SPHiNX does not provide any warranty on the information's accuracy and it cannot be held liable for any damages resulting directly or indirectly from the use or disregard of the information provided herewith.

The information contained herein is for general information purposes only. The information is provided by ETI-SPHiNX and, as we endeavor to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the herein mentioned providers or the information, products, or services. Any reliance you place on such information is therefore strictly at your own risk. To the extent permitted by law, ETI-SPHiNX disclaims all representations and warranties, whether express, implied, statutory, or otherwise, including the warranties of the merchantability, fitness for a particular purpose, title and non-infringement.

---

[1] For HPE Virtual TapeServer (aka VTS), follow appropriate HPE channel to obtain the appropriate software, firmware and procedure to mitigate Meltdown\Spectre CPU vulnerability.

Without limiting the scope of the limitations of liability in ETI-SPHiNX's software license agreement, in no event will ETI-SPHiNX be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of the stated information.

DOCUMENT CHANGES:

3/8/18

- CVSS scores updated
- BIOS availability list: SPHiNX WS, NS, CS, ES and SPHiNX DL380p Gen8

5/24/18

- BIOS availability list: SPHiNX 3U-s, 3U-ns

6/8/18

- Add information about Kernel Side-Channel Attack using Speculative Store Bypass: CVE-2018-3639 (Variant 4)
- Add information about and CVE-2018-3640 – Rogue System Register Load (Variant 3a)
- CVSS scores updated
- No BIOS update for SPHiNX 1U-s, 2U, 2U-s, 3U and 3U-n

6/26/18

- SPHiNX DL380p Gen8 ROM availability for CVE-2018-3639 and CVE-2018-3640 (Variant 4 and 3a)

6/29/18

- SPHiNX WS BIOS availability for CVE-2018-3639 and CVE-2018-3640 (Variant 4 and 3a)

1/2/19

- SPHiNX CS-ES-NS BIOS availability for CVE-2018-3639 and CVE-2018-3640 (Variant 4 and 3a)
- L1 Terminal Fault (CVE-2018-3615, CVE-2018-3620 and CVE-2018-3646)
- 9.6 availability

DETAILED DESCRIPTION:

On January, the 3rd, 2018, side-channel security vulnerabilities involving speculative execution were publicly disclosed by the processors manufacturers (Intel, AMD, etc.). The security vulnerabilities, commonly known as Meltdown and Spectre, allow private data to be read. Server running SPHiNX appliance are affected by these security vulnerabilities.

The CVSS scores given to these vulnerabilities are:

CVE	Scoring system	Base Vector	Base Score
CVE-2017-5715 – aka Spectre, branch target injection (variant #1)	CVSS v3.0	AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.5
	CVSS v2.0	AV:L/AC:M/Au:N/C:C/I:N/A:N	4.7
CVE-2017-5753 – aka Spectre, bounds check bypass (variant #2)	CVSS v3.0	AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.5
	CVSS v2.0	AV:L/AC:M/Au:N/C:C/I:N/A:N	4.7
CVE-2017-5754 – aka Meltdown, rogue data cache load (variant #3)	CVSS v3.0	AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:NN	5.5
	CVSS v2.0	AV:L/AC:M/Au:N/C:C/I:N/A:N	4.7
CVE-2018-3639 – aka Speculative Store Bypass (variant #4)	CVSS v3.0	AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N	4.3
	CVSS v2.0	AV:L/AC:L/Au:N/C:P/I:N/A:N	2.1
CVE-2018-3640 – aka Rogue System Register Load (variant 3a)	CVSS v3.0	AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N	4.3
	CVSS v2.0	AV:L/AC:L/Au:N/C:P/I:N/A:N	2.1
CVE-2018-3615– aka L1 Terminal Fault – L1TF SGX	CVSS v3.0	AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N	6.4
	CVSS v2.0	AV:L/AC:M/Au:N/C:C/I:P/A:N	4.7
CVE-2018-3620– aka L1 Terminal Fault – L1TF SMM	CVSS v3.0	AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6
	CVSS v2.0	AV:L/AC:M/Au:N/C:C/I:N/A:N	4.7
CVE-2018-3646 – aka L1 Terminal Fault – L1TF VMM	CVSS v3.0	AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6
	CVSS v2.0	AV:L/AC:L/Au:N/C:P/I:N/A:N	4.7

For additional and more detailed information on CVSS, see the Forum for Incident Response and Security Teams (FIRST) documents available at https://www.first.org/cvss.

The CVSS guide describes in detail the scoring system. Base scores range from 0 (lowest intrinsic vulnerability) to 10 (highest intrinsic vulnerability).

Intel Security Advisory INTEL-SA-00088 describes Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method - https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00088.html

Intel Security Advisory INTEL-SA-00115 describes Q2 2018 Speculative Execution Side Channel Update - https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html

Intel Security Advisory INTEL-SA-00161 describes L1 Terminal Fault -- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html

For x86 servers running CentOS 6, CentOS has updated the kernel according to Security update released by Red Hat Enterprise Linux 6 OS patches to mitigate the vulnerabilities. The specified CentOS security updates are automatically installed when UPDATING the SPHiNX appliance to the version 9.5.

For variant #1, #2 and #3, general overview can be found at:
https://access.redhat.com/security/vulnerabilities/speculativeexecution

CentOS Errata and Security Advisory 2018:0008 Important
Upstream details at: https://access.redhat.com/errata/RHSA-2018:0008
CentOS Errata and Security Advisory 2018:0013 Important
Upstream details at: https://access.redhat.com/errata/RHSA-2018:0030

The full vulnerabilities mitigation will also require a server system ROM (BIOS) firmware update for the variant #2 of Spectre. Please refer to the server manufacturer for the correct firmware and for the procedure to follow for the BIOS update.

For variant #4, general overview can be found at:
https://access.redhat.com/security/vulnerabilities/ssbd

CentOS Errata and Security Advisory 2018:1651 Important
Upstream details at: https://access.redhat.com/errata/RHSA-2018:1651
CentOS Errata and Security Advisory 2018:1669 Important
Upstream details at: https://access.redhat.com/errata/RHSA-2018:1669

The full vulnerabilities mitigation will also require a server system ROM (BIOS) firmware update for the variant #4 of Speculative Store Bypass. Please refer to the server manufacturer for the correct firmware and for the procedure to follow for the BIOS update.

For variant #3a, only the system ROM (BIOS) firmware update will address this issue.

For L1TF, no new BIOS update is required. General overview can be found at:
https://access.redhat.com/security/vulnerabilities/L1TF

CentOS Errata and Security Advisory 2018:2675 Enhancement Update
Upstream details at: https://access.redhat.com/errata/RHEA-2018:2675
CentOS Errata and Security Advisory 2018:2390 Important
Upstream details at: https://access.redhat.com/errata/RHSA-2018:2390

ADDITIONAL BACKGROUND INFORMATION:

The NIST National Vulnerability Database references are:
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2017-5715
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2017-5753
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2017-5754
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2018-3639
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2018-3640
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2018-3615
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2018-3620
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2018-3646

AFFECTED PRODUCTS:

The affected products are all SPHiNX appliances and branded OEM Virtual TapeServer at version below 9.5-32. Variant #1, #2 and #3 are mitigated from version 9.5-32. Variant #4 is mitigated from version 9.5-33. L1TF are mitigated from version 9.6-18.

For SPHiNX 1U-s, 2U, 2U-s, 3U, and 3U-n, 9.5-33 and above will be required to mitigate Variant #2 via the Retpoline Kernel implantation. For all models, we recommend an upgrade to **9.6-18**.

We suggest planning security fix implementation of the 4 variants in two separate phases:

1. First upgrade the SPHiNX software version to 9.6 and then
2. Schedule a BIOS upgrade when BIOS microcode update is available from the manufacturer.

How to get SPHiNX version 9.6

Use your support credentials to download SPHiNX Software and Documentation from https://sftp.etinet.com under the SPHiNX folder. If you don't have access to your credentials, contact support-sphinx@etinet.com

IMPORTANT: Read the **Release Notes** before starting upgrading to the 9.6 appliance version.

How to identify the SPHiNX model and version

Log in on SPHiNX UI and click the “About” link. Current software version and model (Hardware Platform) can be found in the “About SPHiNX” information box.

How to identify the SPHiNX BIOS version

Open an **ssh** session with the SPHiNX using “bill” credentials and issue the following command to pull out the necessary information:

sudo dmidecode --type bios

```
[bill@vts43 ~]$ sudo dmidecode --type BIOS information
# dmidecode 2.12
SMBIOS 3.0 present.
# SMBIOS implementations newer than version 2.8 are not
# fully supported by this version of dmidecode.

Handle 0x0000, DMI type 0, 24 bytes
BIOS Information
        Vendor: American Megatrends Inc.
        Version: 2.0a
        Release Date: 06/30/2016
        Address: 0xF0000
        Runtime Size: 64 kB
        ROM Size: 8192 kB
        Characteristics:
                PCI is supported
                BIOS is upgradeable
                BIOS shadowing is allowed
                Boot from CD is supported
                Selectable boot is supported
                BIOS ROM is socketed
                EDD is supported
                5.25"/1.2 MB floppy services are supported (int 13h)
                3.5"/720 kB floppy services are supported (int 13h)
                3.5"/2.88 MB floppy services are supported (int 13h)
                Print screen service is supported (int 5h)
                8042 keyboard services are supported (int 9h)
                Serial services are supported (int 14h)
                Printer services are supported (int 17h)
                ACPI is supported
                USB legacy is supported
                BIOS boot specification is supported
                Targeted content distribution is supported
                UEFI is supported
        BIOS Revision: 5.11

Handle 0x008D, DMI type 13, 22 bytes
BIOS Language Information
        Language Description Format: Long
        Installable Languages: 1
                en|US|iso8859-1
        Currently Installed Language: en|US|iso8859-1

[bill@vts43 ~]$
```

How to get the SPHiNX BIOS update

Once you identified your SPHiNX model, use the table below to find out which Manufacturer Model and which BIOS version is needed. Use the provided link to download the required BIOS.

If your SPHiNX model is not listed in the table below, this means that your server type has reached is End Of Life support and no BIOS update has been planned from server vendors. In this case, to get full mitigation on Spectre and Meltdown, please contact ETI-SPHiNX sales representative to replace your appliance.

SPHiNX model (aka UI - hardware platform)	Manufacturer	Manufacturer model (aka UI - server type)	CPU type	BIOS/ROM Current version	BIOS/ROM patch availability	
					Variant #2	Variant #4
SPHiNX 1U-s **SPHiNX 2U** **SPHiNX 2U-s**	Supermicro	**X7DCU**	Intel® Xeon® Processor L5410	1.2b	NO PATCH	NO PATCH EXPECT
SPHiNX 3U **SPHiNX 3U-n**	Supermicro	**X7DB8**	Intel® Xeon® Processor L5410	2.1c	NO PATCH	NO PATCH EXPECT
After a comprehensive investigation of the microarchitectures and microcode capabilities for these products, Intel has determined to not release microcode updates for these products for one or more reasons including, but not limited to the following: • Micro-architectural characteristics that preclude a practical implementation of features mitigating Variant 2 (CVE-2017-5715) • Limited Commercially Available System Software support • Based on customer inputs, most of these products are implemented as "closed systems" and therefore are expected to have a lower likelihood of exposure to these vulnerabilities.						
SPHiNX 3U-s **SPHiNX 3U-ns**	Supermicro	**X8DTH-iF**	Intel® Xeon® Processor 5600, 5500 Series	2.1b patched with the Update Tool	AVAILABLE	NO PATCH EXPECT
SPHiNX WS	Supermicro	**X10SRL-F**	Intel® Xeon® Processor E5-1600 v4/v3 family	3.1	AVAILABLE	AVAILABLE
SPHiNX CS **SPHiNX ES** **SPHiNX NS**	Supermicro	**X10DRH-iT**	Intel® Xeon® Processor E5-2600 v4/v3 family	3.1	AVAILABLE	AVAILABLE
For all SPHiNX Supermicro (1U-s, 2U, 2U-s, 3U, 3U-n, 3U-s, 3U-ns, WS, CS, ES and NS) Use your support credentials to download SPHiNX Supermicro BIOS update kit ISO from **https://sftp.etinet.com** under the SPHiNX folder. If you don't have access to your credentials, contact support-sphinx@etinet.com						
SPHINX	HPE	**DL380p Gen8**	Intel® Xeon® Processor E5-2600 v2 family	P70 2018.05.21 (25 Jun 2018)	AVAILABLE	AVAILABLE
Download P70 2018.05.21 ROM : **https://support.hpe.com/hpsc/swd/public/detail?swItemId=MTX_bc66ddcd4740483a9d0eaa165c**						

ADDITIONAL MANUFACTURER SIDE-CHANNEL SECURITY VULNERRABILITIES INFORMATION:

For Supermicro:
https://www.supermicro.com/support/security_Intel-SA-00088.cfm

For HPE:

https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00039267en_us
https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03850en_us

How to verify if SPHiNX is mitigated for Meltdown and Spectre vulnerabilities

Verification script can be downloaded from Red Hat web site:
https://access.redhat.com/security/vulnerabilities/speculativeexecution.
You will found the script into the Diagnose section. Click on the link detection script to download it.

To validate if VTS ROM and OS have been mitigated, follow the procedure:

1- Upload the downloaded script on the SPHiNX
2- Start an ssh session with the SPHiNX using bill credentials
3- From the prompt log in as root
4- Go to the folder where the script has been uploaded
5- Change the script permissions to allow execution

```
chmod 770 spectre-meltdown--xxxxxxx.sh
```

6- Mount the following drive

```
mount -t debugfs nodev /sys/kernel/debug
```

7- Execute the verification script. If ROM has been patched, variant #2 would be green, marked with the flag “Mitigated”. To run the verification script, use the following command:

```
./spectre-meltdown--xxxxxxx.sh
```

8- Once the verification is done, unmount the drive before quitting:

```
umount /sys/kernel/debug
```

The output example below shows the result of a server with the BIOS/ROM not patched:

```
[root@vts28 bill]# mount -t debugfs nodev /sys/kernel/debug
[root@vts28 bill]# # ./spectre-meltdown--2018-05-23-1220.sh

Spectre/Meltdown Detection Script Ver. 2.6
This script is primarily designed to detect Spectre / Meltdown on supported
Red Hat Enterprise Linux systems and kernel packages.
Result may be inaccurate for other RPM based systems.

Detected CPU vendor: Intel
Running kernel: 2.6.32-696.30.1.el6.x86_64

Variant #1 (Spectre): Mitigation: Load fences
CVE-2017-5753 - speculative execution bounds-check bypass
   - Kernel with mitigation patches: OK

Variant #2 (Spectre): Mitigation: Full retpoline
CVE-2017-5715 - speculative execution branch target injection
   - Kernel with mitigation patches: OK
   - HW support / updated microcode: YES
   - IBRS: Not disabled on kernel commandline
   - IBPB: Not disabled on kernel commandline
   - Retpolines: Not disabled on kernel commandline

Variant #3 (Meltdown): Mitigation: PTI
CVE-2017-5754 - speculative execution permission faults handling
   - Kernel with mitigation patches: OK
   - PTI: Not disabled on kernel commandline

Note about virtualization
In virtualized environment, there are more steps to mitigate the issue,
including:
* Host needs to have updated kernel and CPU microcode
* Host needs to have updated virtualization software
* Guest needs to have updated kernel
* Hypervisor needs to propagate new CPU features correctly
For more details about mitigations in virtualized environment see:
https://access.redhat.com/articles/3331571

For more information about the vulnerabilities see:
https://access.redhat.com/security/vulnerabilities/speculativeexecution

[root@vts28 bill]# umount /sys/kernel/debug
[root@vts28 bill]#
```

How to verify if SPHiNX is mitigated for Kernel Side-Channel Attack using Speculative Store Bypass

Verification script can be downloaded from Red Hat web site:
https://access.redhat.com/security/vulnerabilities/ssbd.
You will found the script into the Diagnose section. Click on the link detection script to download it.

To validate if VTS ROM and OS have been mitigated, follow the procedure:

1- Upload the downloaded script on the SPHiNX
2- Start an ssh session with the SPHiNX using “bill” credentials
3- From the prompt log in as root
4- Go to the folder where the script has been uploaded
5- Change the script permissions to allow execution

```
chmod 770 cve-2018-3639--XXXX-XX-XX-XXXX.sh
```

6- Execute the verification script. If ROM has been patched, variant #2 would be green, marked with the flag “Mitigated”. To run the verification script, use the following command:

```
./cve-2018-3639--XXXX-XX-XX-XXXX.sh
```

```
[root@vts28 bill]# ./cve-2018-3639--2018-05-21-1502.sh

This script (v1.0) is primarily designed to detect CVE-2018-3639 on supported
Red Hat Enterprise Linux systems and kernel packages.
Result may be inaccurate for other RPM based systems.

This system is vulnerable for the following reasons:
* CPU microcode is not updated

Follow https://access.redhat.com/security/vulnerabilities/ssbd for advice.
[root@vts28 bill]#
```

The output example above shows the result of a server with the BIOS/ROM not patched.

How to verify if SPHiNX is mitigated for L1 Terminal Fault (L1TF) – SGX, SMM and VMM):

A verification script can be downloaded from the Red Hat web site: https://access.redhat.com/security/vulnerabilities/L1TF.

You will find the script in the "Diagnose" section. Click on the button DOWNLOAD DETECTION SCRIPT at the end of the page.

To validate if OS has been mitigated, follow the procedure:

1- Upload the downloaded script on the SPHiNX.
2- Start a ssh session with the SPHiNX.
3- At the prompt, log as root.
4- Go to the folder containing the verification script.
5- Change the script permission to allow execution.

```
chmod 770 cve-2018-3620--XXXX-XX-XX-XXXX.sh
```

6- Execute the verification script using the command

```
./cve-2018-3620--XXXX-XX-XX-XXXX.sh
```

The following output example shows the result of a server with all mitigations updated:

```
[root@vts28 bill]# ./ cve-2018-3620--2018-09-06-0736.sh

CVE-2018-3620 Detection Script Ver. 1.3
This script is primarily designed to detect CVE-2018-3620 on Supported
Red Hat Enterprise Linux systems and kernel packages.
Result may be inaccurate for other RPM based systems..

CPU vendor: Intel
Running kernel: 2.6.32-754.3.5.el6.x86_64
Virtualization: None
SMT status: On
Mitigation: Mitigation: PTE Inversion

This system is not vulnerable, because it has correct mitigation
applied.

Note about Hyper-Threading (SMT)
Customers desiring to completely mitigate this issue will need to consider disabling
SMT.
For details how to disable SMT see:
https://access.redhat.com/solutions/352663

[root@vts28 bill]#
```