Initial Publication: 1/18/18 7:47:00 AM
Last Update: 1/26/18 3:59:00 PM

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.

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.

---

[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.

DETAILED DESCRIPTION:

On January, the 3rd, 2018, side-channel security vulnerabilities involving speculative execution were publicly disclosed by the processors manufacturer (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:A/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N	8.2
	CVSS v2.0	AV:A/AC:L/Au:N/C:C/I:P/A:N	6.8
CVE-2017-5753 – aka Spectre, bounds check bypass (variant #2)	CVSS v3.0	AV:A/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L	5.0
	CVSS v2.0	AV:A/AC:L/Au:N/C:C/I:P/A:N	5.4
CVE-2017-5754 – aka Meltdown, rogue data cache load (variant #3)	CVSS v3.0	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
	CVSS v2.0	AV:N/AC:L/Au:N/C:C/I:N/A:N	7.8

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 the security vulnerabilities affecting specific Intel x86 processors - https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

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.

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 procedure to follow for the BIOS update.

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

AFFECTED PRODUCTS:

The affected products are all SPHiNX appliances and branded OEM Virtual TapeServer at version below 9.5.

Since CVE base score for variant #2 is less than the one for variants #1 and #3, we suggest planning security fix implementation of the 3 variants in two separate phases:

1. First upgrade the SPHiNX software version to 9.5 and
2. Then schedule a BIOS upgrade when BIOS becomes available.

How to get SPHiNX version 9.5

As soon as SPHiNX 9.5 is released a notification will be sent to all customers and partners using SPHiNX appliances.

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 9.5 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 ollowing 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. As of today, vendors have not released yet a BIOS update required for microcode updates. As the vendor's BIOS update has not been yet released, ETI-SPHiNX cannot be held responsible for any BIOS-related issues.

However, ETI-SPHiNX is committed to keep looking for new BIOS releases. We will constantly update the BIOS information listed in the table below and we will let you know as soon as any information becomes available.

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 yet 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 version for full mitigation	BIOS availability
SPHiNX3U-s	SuperMicro	**X8DTH-i/6/iF/6F**	Intel® Xeon® Processor 5600, 5500 Series	N/A	PENDING
SPHiNX3U-ns	SuperMicro	**X8DTH-i/6/iF/6F**	Intel® Xeon® Processor 5600, 5500 Series	N/A	PENDING
SPHiNX-WS	SuperMicro	**X10SRL-F**	Intel® Xeon® Processor E5-2600 v4 / v3, E5-1600 v4 / v3 family	N/A	PENDING
SPHiNX-CS	SuperMicro	**X10DRH-iT**	Intel® Xeon® Processor E5-2600 v4 / v3 family	N/A	PENDING
SPHiNX-ES	SuperMicro	**X10DRH-iT**	Intel® Xeon® Processor E5-2600 v4 / v3 family	N/A	PENDING
SPHiNX-NS	SuperMicro	**X10DRH-iT**	Intel® Xeon® Processor E5-2600 v4 / v3 family	N/A	PENDING
SPHINX	HPE	**DL380p Gen8**	Intel® Xeon® Processor E5-2600 v2 family	N/A	PENDING

Depending on your SPHiNX model manufacturer, select the appropriate link to find the BIOS and follow the BIOS upgrade instructions.

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

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 has 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 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 have been patched, variant #2 would be green 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 above output example shows the result of a server with the ROM not patched:

```
[root@vts28 bill]# mount -t debugfs nodev /sys/kernel/debug
[root@vts28 bill]# # ./spectre-meltdown--23ef32a.sh

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: 2.6.32-696.18.7.el6.x86_64

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

Variant #2 (Spectre): Vulnerable
CVE-2017-5715 - speculative execution branch target injection
   - Kernel with mitigation patches: OK
   - HW support / updated microcode: NO
   - IBRS: Not disabled on kernel commandline
   - IBPB: Not disabled on kernel commandline

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

Red Hat recommends that you:
* Ask your HW vendor for CPU microcode update.

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

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