Department of Homeland Security (DHS)
Enterprise Security Operations Center (ESOC)
Vulnerability Assessment Team (VAT)
Information Security Vulnerability Management (ISVM)

ISVM Title: 2018-408781-0-TA-Meltdown Vulnerability

CVE Number:
CVE-2017-5754

Severity: High

Acknowledgement Required: No
Compliance Response Required: No
Release Date: 01/04/2018

Revision Summary: N/A

Type of Systems Affected:
- Databases
- Networking
- Servers
- Workstations

Platform Affected (*additional platforms may apply):
- Windows
- Linux
- Unix
- Mac OS

Products & Version Affected:

Potential Impact of Threat:

Impact to Systems

- All DHS hardware containing Intel chipsets are vulnerable to the Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5715 and CVE-2017-5753) vulnerabilities.
- All DHS hardware containing AMD/ARM chipsets are vulnerable to the Spectre vulnerability.

Current Mitigation
Microsoft has released a patch (ADV180002) to mitigate the Meltdown and Spectre Vulnerabilities

Note Current patch fixes by Microsoft may degrade performance of the processor anywhere from 5%-30%. Microsoft also warns the patch affects AV solutions. It is recommended that components perform testing before applying patches to machines utilizing a risk-based approach.

ARM

Processor	Variant 1	Variant 2	Variant 3	Variant 3a
Cortex-R7	Yes*	Yes*	No	No
Cortex-R8	Yes*	Yes*	No	No
Cortex-A8	Yes (under review)	Yes	No	No
Cortex-A9	Yes	Yes	No	No
Cortex-A15	Yes (under review)	Yes	No	Yes
Cortex-A17	Yes	Yes	No	No
Cortex-A57	Yes	Yes	No	Yes
Cortex-A72	Yes	Yes	No	Yes
Cortex-A73	Yes	Yes	No	No
Cortex-A75	Yes	Yes	Yes	No

* Note for Cortex-R cores: The common usage model for Cortex-R is in non-open environments where applications or processes are strictly controlled and hence not exploitable.

Microsoft

Product	Platform	Article	Download	Supersedence
Internet Explorer 11	Windows 10 Version 1703 for 32-bit Systems	4056891	Security Update	4053580
Internet Explorer 11	Windows 10 Version 1703 for x64-based Systems	4056891	Security Update	4053580
Internet Explorer 11	Windows 10 Version 1709 for 32-bit Systems	4056892	Security Update	4054517
Internet Explorer 11	Windows 10 Version 1709 for 64-based Systems	4056892	Security Update	4054517
Internet Explorer 11	Windows 10 for 32-bit Systems	4056893	Security Update	4053581
Internet Explorer 11	Windows 10 for x64-based Systems	4056893	Security Update	4053581
Internet Explorer 11	Windows 10 Version 1511 for 32-bit Systems	4056893	Security Update	4053581
Internet Explorer 11	Windows 10 Version 1511 for x64-based Systems	4056893	Security Update	4053581
Internet Explorer 11	Windows 10 Version 1607 for 32-bit Systems	4056890	Security Update	4053579
Internet Explorer 11	Windows 10 Version 1607 for x64-based Systems	4056890	Security Update	4053579
Internet Explorer 11	Windows Server 2016	4056890	Security Update	4053579
Internet Explorer 11	Windows 7 for 32-bit Systems	4056568	IE Cumulative	4052978

	Service Pack 1			
Internet Explorer 11	Windows 7 for x64-based Systems Service Pack 1	4056568	IE Cumulative	4052978
Internet Explorer 11	Windows 8.1 for 32-bit systems	4056568	IE Cumulative	4052978
Internet Explorer 11	Windows 8.1 for x64-based systems	4056568	IE Cumulative	4052978
Internet Explorer 11	Windows Server 2008 R2 for x64-based Systems Service Pack 1	4056568	IE Cumulative	4052978
Internet Explorer 11	Windows Server 2012 R2	4056568	IE Cumulative	4052978
Microsoft Edge	Windows 10 Version 1703 for 32-bit Systems	4056891	Security Update	4053580
Microsoft Edge	Windows 10 Version 1703 for x64-based Systems	4056891	Security Update	4053580
Microsoft Edge	Windows 10 Version 1709 for 32-bit Systems	4056892	Security Update	4054517
Microsoft Edge	Windows 10 Version 1709 for 64-based Systems	4056892	Security Update	4054517
Microsoft Edge	Windows 10 for 32-bit Systems	4056893	Security Update	4053581
Microsoft Edge	Windows 10 for x64-based Systems	4056893	Security Update	4053581
Microsoft Edge	Windows 10 Version 1511 for 32-bit Systems	4056888	Security Update	4053578
Microsoft Edge	Windows 10 Version 1511 for x64-based Systems	4056888	Security Update	4053578
Microsoft Edge	Windows 10 Version 1607 for 32-bit Systems	4056890	Security Update	4053579
Microsoft Edge	Windows 10 Version 1607 for x64-based Systems	4056890	Security Update	4053579
Microsoft Edge	Windows Server 2016	4056890	Security Update	4053579
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1		4057118	Security Update	
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (CU)		4057119	Security Update	
Microsoft SQL Server 2017 for x64-based Systems		4057122	Security Update	
Microsoft SQL Server 2017 for x64-based Systems (CU)		4052987	Security Update	

Windows 10 for 32-bit Systems		4056893	Security Update	4053581
Windows 10 for x64-based Systems		4056893	Security Update	4053581
Windows 10 Version 1511 for 32-bit Systems		4056888	Security Update	4053578
Windows 10 Version 1511 for x64-based Systems		4056888	Security Update	4053578
Windows 10 Version 1607 for 32-bit Systems		4056890	Security Update	4053579
Windows 10 Version 1607 for x64-based Systems		4056890	Security Update	4053579
Windows 10 Version 1703 for 32-bit Systems		4056891	Security Update	4053580
Windows 10 Version 1703 for x64-based Systems		4056891	Security Update	4053580
Windows 10 Version 1709 for 32-bit Systems		4056892	Security Update	4054517
Windows 7 for 32-bit Systems Service Pack 1		4056897	Security Only	
Windows 7 for x64-based Systems Service Pack 1		4056897	Security Only	
Windows 8.1 for 32-bit systems		4056898	Security Only	
Windows 8.1 for x64-based systems		4056898	Security Only	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1		4056897	Security Only	
Windows Server 2008 R2 for x64-based Systems Service Pack 1		4056897	Security Only	
Windows Server 2008 R2 for x64-based Systems Service Pack		4056897	Security Only	

1 (Server Core installation)				
Windows Server 2012		4056899	Security Only	
Windows Server 2012 (Server Core installation)		4056899	Security Only	
Windows Server 2012 R2		4056898	Security Only	
Windows Server 2012 R2 (Server Core installation)		4056898	Security Only	
Windows Server 2016		4056890	Security Update	4053579
Windows Server 2016 (Server Core installation)		4056890	Security Update	4053579
Windows Server, version 1709 (Server Core Installation)		4056892	Security Update	4054517

Redhat

Platform	Package	State	Patch
Red Hat Enterprise MRG 2	kernel-rt	Affected	In-Progress
Red Hat Enterprise Linux 7	kernel-alt	Affected	In-Progress
Red Hat Enterprise Linux 7	kernel	Affected	In-Progress
Red Hat Enterprise Linux 7	kernel-rt	Affected	In-Progress
Red Hat Enterprise Linux 6	kernel	Affected	In-Progress
Red Hat Enterprise Linux 5	kernel	Affected	

SUSE

CVE-2017-5754

Product(s)	Source package	State
SUSE Linux Enterprise Desktop 12 SP2	kernel-source	In progress
SUSE Linux Enterprise Desktop 12 SP3	kernel-source	In progress
SUSE Linux Enterprise Server 11 SP3 LTSS	kernel-source	In progress
SUSE Linux Enterprise Server 11 SP4	kernel-source	In progress
SUSE Linux Enterprise Server 12 GA LTSS	kernel-source	In progress
SUSE Linux Enterprise Server 12 SP1 LTSS	kernel-source	In progress
SUSE Linux Enterprise Server 12 SP2	kernel-source	In progress
SUSE Linux Enterprise Server 12 SP3	kernel-source	In progress

Patch Number(s):

Potential Impact of Threat:

Impact to Systems

- All DHS hardware containing Intel chipsets are vulnerable to the Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5715 and CVE-2017-5753) vulnerabilities.
- All DHS hardware containing AMD/ARM chipsets are vulnerable to the Spectre vulnerability.

Current Mitigation

Microsoft has released a patch (ADV180002) to mitigate the Meltdown and Spectre Vulnerabilities
Note Current patch fixes by Microsoft may degrade performance of the processor anywhere from 5%-30%. Microsoft also warns the patch affects AV solutions. It is recommended that components perform testing before applying patches to machines utilizing a risk-based approach.

ARM

Step 1

Check the table below to determine if you have an affected processor.

- Only affected cores are listed, **all other Arm cores are NOT affected**.
- **No** indicates not affected by the particular variant.
- **Yes** indicates affected by the particular variant but has a mitigation (unless otherwise stated).

Processor	Variant 1	Variant 2	Variant 3	Variant 3a
Cortex-R7	Yes*	Yes*	No	No
Cortex-R8	Yes*	Yes*	No	No
Cortex-A8	Yes (under review)	Yes	No	No
Cortex-A9	Yes	Yes	No	No
Cortex-A15	Yes (under review)	Yes	No	Yes
Cortex-A17	Yes	Yes	No	No
Cortex-A57	Yes	Yes	No	Yes
Cortex-A72	Yes	Yes	No	Yes
Cortex-A73	Yes	Yes	No	No
Cortex-A75	Yes	Yes	Yes	No

* Note for Cortex-R cores: The common usage model for Cortex-R is in non-open environments where applications or processes are strictly controlled and hence not exploitable.

Step 2

- If you are running Linux, please follow the directions below according to the variant identified in the table.
- If you are running Android, please check with Google for the detail of supported kernel versions.
- If you are running another OS, please contact the OS vendor for details.
- For JIT development, check the generated code and replace with new instruction sequences as detailed in the Cache Speculation Side-channels whitepaper.

For Linux

Variant 1

Action required:

- Search your code for the code snippets as described in the Cache Speculation Side-channels whitepaper.
- Once identified use the compiler support for mitigations as described in Compiler support for mitigations to modify your code, and recompile using an updated compiler.

Variant 2

The mitigation will vary by processor micro-architecture:

For Cortex-A57 and Cortex-A72:

- Apply all kernel patches provided by Arm and available at https://git.kernel.org/pub/scm/linux/kernel/git/arm64/linux.git/log/?h=kpti
- Also apply all Arm Trusted Firmware patches.

For Cortex-A73:

- Apply all kernel patches provided by Arm and available at https://git.kernel.org/pub/scm/linux/kernel/git/arm64/linux.git/log/?h=kpti
- Also apply all Arm Trusted Firmware patches.

For Cortex-A75:

- Apply all kernel patches provided by Arm and available at https://git.kernel.org/pub/scm/linux/kernel/git/arm64/linux.git/log/?h=kpti
- Also apply all Arm Trusted Firmware patches.

Variant 3

For Cortex-A75:

- Apply all kernel patches provided by Arm and available at https://git.kernel.org/pub/scm/linux/kernel/git/arm64/linux.git/log/?h=kpti
- There is no need to further check or modify code outside of kernel code.

Variant 3a

For Cortex-A15, Cortex-A57, and Cortex-A72:

- In general, it is not believed that software mitigations for this issue are necessary. Please download the Cache Speculation Side-channels whitepaper for more details.

Microsoft

Product	Platform	Article	Download	Supersedence
Internet Explorer 11	Windows 10 Version 1703 for 32-bit Systems	4056891	Security Update	4053580
Internet Explorer 11	Windows 10 Version 1703 for x64-based Systems	4056891	Security Update	4053580
Internet Explorer 11	Windows 10 Version 1709 for 32-bit Systems	4056892	Security Update	4054517
Internet Explorer 11	Windows 10 Version 1709 for 64-based Systems	4056892	Security Update	4054517
Internet Explorer 11	Windows 10 for 32-bit Systems	4056893	Security Update	4053581
Internet Explorer 11	Windows 10 for x64-based Systems	4056893	Security Update	4053581
Internet Explorer 11	Windows 10 Version 1511 for 32-bit Systems	4056893	Security Update	4053581
Internet Explorer 11	Windows 10 Version 1511 for x64-based Systems	4056893	Security Update	4053581
Internet Explorer 11	Windows 10 Version 1607 for 32-bit Systems	4056890	Security Update	4053579
Internet Explorer 11	Windows 10 Version 1607 for x64-based Systems	4056890	Security Update	4053579
Internet Explorer 11	Windows Server 2016	4056890	Security Update	4053579
Internet Explorer 11	Windows 7 for 32-bit Systems Service Pack 1	4056568	IE Cumulative	4052978
Internet Explorer 11	Windows 7 for x64-based Systems Service Pack 1	4056568	IE Cumulative	4052978
Internet Explorer 11	Windows 8.1 for 32-bit systems	4056568	IE Cumulative	4052978
Internet Explorer 11	Windows 8.1 for x64-based systems	4056568	IE Cumulative	4052978
Internet Explorer 11	Windows Server 2008 R2 for x64-based Systems Service Pack 1	4056568	IE Cumulative	4052978
Internet Explorer 11	Windows Server 2012 R2	4056568	IE Cumulative	4052978
Microsoft Edge	Windows 10 Version 1703 for 32-bit Systems	4056891	Security Update	4053580
Microsoft Edge	Windows 10 Version 1703 for x64-based Systems	4056891	Security Update	4053580
Microsoft Edge	Windows 10 Version 1709 for 32-bit Systems	4056892	Security Update	4054517
Microsoft Edge	Windows 10 Version 1709 for 64-based Systems	4056892	Security Update	4054517

Microsoft Edge	Windows 10 for 32-bit Systems	4056893	Security Update	4053581
Microsoft Edge	Windows 10 for x64-based Systems	4056893	Security Update	4053581
Microsoft Edge	Windows 10 Version 1511 for 32-bit Systems	4056888	Security Update	4053578
Microsoft Edge	Windows 10 Version 1511 for x64-based Systems	4056888	Security Update	4053578
Microsoft Edge	Windows 10 Version 1607 for 32-bit Systems	4056890	Security Update	4053579
Microsoft Edge	Windows 10 Version 1607 for x64-based Systems	4056890	Security Update	4053579
Microsoft Edge	Windows Server 2016	4056890	Security Update	4053579
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1		4057118	Security Update	
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (CU)		4057119	Security Update	
Microsoft SQL Server 2017 for x64-based Systems		4057122	Security Update	
Microsoft SQL Server 2017 for x64-based Systems (CU)		4052987	Security Update	
Windows 10 for 32-bit Systems		4056893	Security Update	4053581
Windows 10 for x64-based Systems		4056893	Security Update	4053581
Windows 10 Version 1511 for 32-bit Systems		4056888	Security Update	4053578
Windows 10 Version 1511 for x64-based Systems		4056888	Security Update	4053578
Windows 10 Version 1607 for 32-bit Systems		4056890	Security Update	4053579
Windows 10 Version 1607 for x64-based Systems		4056890	Security Update	4053579
Windows 10 Version 1703 for 32-bit Systems		4056891	Security Update	4053580

Windows 10 Version 1703 for x64-based Systems		4056891	Security Update	4053580
Windows 10 Version 1709 for 32-bit Systems		4056892	Security Update	4054517
Windows 7 for 32-bit Systems Service Pack 1		4056897	Security Only	
Windows 7 for x64-based Systems Service Pack 1		4056897	Security Only	
Windows 8.1 for 32-bit systems		4056898	Security Only	
Windows 8.1 for x64-based systems		4056898	Security Only	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1		4056897	Security Only	
Windows Server 2008 R2 for x64-based Systems Service Pack 1		4056897	Security Only	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)		4056897	Security Only	
Windows Server 2012		4056899	Security Only	
Windows Server 2012 (Server Core installation)		4056899	Security Only	
Windows Server 2012 R2		4056898	Security Only	
Windows Server 2012 R2 (Server Core installation)		4056898	Security Only	
Windows Server 2016		4056890	Security Update	4053579
Windows Server 2016 (Server Core installation)		4056890	Security Update	4053579
Windows Server, version 1709 (Server Core Installation)		4056892	Security Update	4054517

Redhat

Platform	Package	State	Patch
Red Hat Enterprise MRG 2	kernel-rt	Affected	In-Progress
Red Hat Enterprise Linux 7	kernel-alt	Affected	In-Progress
Red Hat Enterprise Linux 7	kernel	Affected	In-Progress
Red Hat Enterprise Linux 7	kernel-rt	Affected	In-Progress
Red Hat Enterprise Linux 6	kernel	Affected	In-Progress
Red Hat Enterprise Linux 5	kernel	Affected	

SUSE

CVE-2017-5754

Product(s)	Source package	State
SUSE Linux Enterprise Desktop 12 SP2	kernel-source	In progress
SUSE Linux Enterprise Desktop 12 SP3	kernel-source	In progress
SUSE Linux Enterprise Server 11 SP3 LTSS	kernel-source	In progress
SUSE Linux Enterprise Server 11 SP4	kernel-source	In progress
SUSE Linux Enterprise Server 12 GA LTSS	kernel-source	In progress
SUSE Linux Enterprise Server 12 SP1 LTSS	kernel-source	In progress
SUSE Linux Enterprise Server 12 SP2	kernel-source	In progress
SUSE Linux Enterprise Server 12 SP3	kernel-source	In progress

Vendor Patches

Meltdown
ARM – https://developer.arm.com/support/security-update
Microsoft – https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002
RedHat - https://access.redhat.com/solutions/3307791
https://access.redhat.com/articles/3307751
https://access.redhat.com/solutions/3307851
SUSE - https://www.suse.com/security/cve/CVE-2017-5754/

Overview:

Multiple Vendors has released security advisories to address vulnerabilities, in which successful local/remote exploitation may result in information disclosure.

Action:

All DHS Components are encouraged to ensure all available updates or workarounds are applied to all affected systems. Components are responsible for any testing necessary to confirm that system changes do not cause a significant negative impact on their systems. Components should take steps to ensure that they have addressed the vulnerability either via a software upgrade or workarounds in place as appropriate in order to mitigate any risk from potential exploitation.

CVE Details:

Total # of CVEs: 1

CVE Number	CVE Details
CVE-2017-5754	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

Additional Information:

Potential Impact of Threat:

Impact to Systems

- All DHS hardware containing Intel chipsets are vulnerable to the Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5715 and CVE-2017-5753) vulnerabilities.
- All DHS hardware containing AMD/ARM chipsets are vulnerable to the Spectre vulnerability.

Current Mitigation
Microsoft has released a patch (ADV180002) to mitigate the Meltdown and Spectre Vulnerabilities
Note Current patch fixes by Microsoft may degrade performance of the processor anywhere from 5%-30%. Microsoft also warns the patch affects AV solutions. It is recommended that components perform testing before applying patches to machines utilizing a risk-based approach.

Official Notices

US-CERT VU#584653 http://www.kb.cert.org/vuls/id/584653
MITRE CVE-2017-5753 https://nvd.nist.gov/vuln/detail/CVE-2017-5753
MITRE CVE-2017-5715 https://nvd.nist.gov/vuln/detail/CVE-2017-5715
MITRE CVE-2017-5754 https://nvd.nist.gov/vuln/detail/CVE-2017-5754

Informational Links

https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html
https://nakedsecurity.sophos.com/2018/01/03/fckwit-aka-kaiser-aka-kpti-intel-cpu-flaw-needs-low-level-os-patches/
https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw
https://arstechnica.com/gadgets/2018/01/whats-behind-the-intel-design-flaw-forcing-numerous-patches/

Vendor Updates

Cloud

Vendor	Link	Last Checked	Updates
MS	https://azure.microsoft.com/en-	1/4/2018	The majority of Azure infrastructure has already

Azure	us/blog/securing-azure-customers-from-cpu-vulnerability/	9:38 AM	updated to address this vulnerability. Some aspe Azure are still being updated and require a reboo customer VMs for the security update to take eff Many of you have received notification in recen of a planned maintenance on Azure and have alr rebooted your VMs to apply the fix, and no furth by you is required.
Amazon AWS	https://aws.amazon.com/security/security-bulletins/AWS-2018-013/	1/4/2018 9:38 AM	All but a small single-digit percentage of instanc the Amazon EC2 fleet are already protected. The remaining ones will be completed in the next sev hours, with associated instance maintenance notifications. While the updates AWS performs underlying infrastructure, in order to be fully pro against these issues, customers must also patch t instance operating systems. Updates for Amazon have been made available, and instructions for u existing instances are provided further below alo any other AWS-related guidance relevant to this

Workstation/Server Operating Systems

Vendor	Link	Last Checked	Updates
MS Windows	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002	1/4/2018 9:38 AM	Updates available for Windows Server, version 1709 (Server Core Installation); Windows Server 2016; Windows Server 2012 R2; Windows Server 2008 R2; Windows 10 (RTM,

			1511, 1607, 1703, 1709), Windows 8.1, Windows 7 SP1 **(NOT Windows Server 2012; Windows Server 2008)**
Redhat	https://access.redhat.com/security/vulnerabilities/speculativeexecution?sc_cid=701f2000000tsLNAAY&	1/4/2018 9:38 AM	Red Hat customers running affected versions of the Red Hat products are strongly recommended to update them as soon as errata are available.
Apple OSX			

Antivirus

Vendor	**Link**	**Last Checked**	**Updates**
Microsoft (Advisory)	https://support.microsoft.com/en-in/help/4072699/important-information-regarding-the-windows-security-updates-released	1/4/2018 10:50 AM	AV Vendors need to set a specific registry key to

			indicate to the Windows OS that they are compatible with the update before it will be served to the endpoint. Windows Defender for Windows 10 and Microsoft Security Essentials for Windows 7 are compatible.
OSINT	https://docs.google.com/spreadsheets/d/184wcDt9I9TUNFFbsAVLpzAtckQxYiuirADzf3cL42FQ/htmlview?sle=true#gid=0	1/4/2018 10:52 AM	Table maintained by independent researcher Kevin Beaumont (@GossiTheDog on twitter) of AV vendor responses
McAfee	N/A	1/4/2018 10:30	McAfee is aware of the issue, and

		AM	is working on it. The engineering team was caught off guard by the unexpected disclosure of these vulnerabilities which were scheduled for release next week. Updates are in the works.
Symantec	https://pbs.twimg.com/media/DSsRaXBVoAEDpMR.jpg:large	1/4/2018 11:00 AM	Symantec deployed an update for their ERASER Engine (117.3.0.358) that makes it compatible with the update from Microsoft for the Windows OS.
Sophos	https://community.sophos.com/kb/en-us/128053	1/4/2018 11:00	Sophos is currently testing this patch

		AM	and registry key, with initial results showing no compatibility issues. Sophos plans to automatically add the registry key early next week, once all tests have been completed.

Hypervisors

Vendor	Link	Last Checked	Updates
VMWare	https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html	1/4/2018 10:36 AM	Updates available for ESXi 5.5, 6.0, 6.5; Workstation 12.x; Fusion 8.x (on OSX) to mitigate CVE-2017-5753, CVE-2017-5715

Chip Manufacturers

Vendor	Link	Last Checked	Updates
Intel	https://newsroom.intel.com/news/intel-responds-to-security-research-findings/	1/4/2018 10:36 AM	Intel believes these exploits do not have the potential to corrupt, modify or delete data. Based on the analysis to date, many types of

			computing devices — with many different vendors' processors and operating systems — are susceptible to these exploits.
AMD	https://www.amd.com/en/corporate/speculative-execution	1/4/2018 11:00 AM	Software solution to CVE-2017-5753 available, not vulnerable to CVE-2017-5715 or CVE-2017-5754
ARM	https://developer.arm.com/support/security-update	1/4/2018 12:08 PM	

Mobile Operating Systems

Vendor	Link	Last Checked	Updates
Apple iOS	N/A	N/A	N/A
Google Android	N/A	N/A	N/A

References:

Proof-of-Concept (PoC)

https://meltdownattack.com/
https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

Vendor Details

Amazon
https://aws.amazon.com/de/security/security-bulletins/AWS-2018-013/
https://alas.aws.amazon.com/ALAS-2018-939.html
Microsoft - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002
Redhat
https://access.redhat.com/security/vulnerabilities/speculativeexecution
SUSE
https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/

Vendor Patches

Meltdown
AMS – https://alas.aws.amazon.com/ALAS-2018-939.html
ARM – https://developer.arm.com/support/security-update
Microsoft – https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002
RedHat - https://access.redhat.com/solutions/3307791
https://access.redhat.com/articles/3307751
https://access.redhat.com/solutions/3307851
SUSE - https://www.suse.com/security/cve/CVE-2017-5754/

Contact Information:

DHS Enterprise Security Operations Center (ESOC)

Phone: 1-877-347-1638 Option 2
Email: DHSESOC@hq.dhs.gov