COMPLIANCE REPORT: CJIS V5.9.5_

Summary

Report Date 2024-08-26

Controls Passed 0
Controls Needs Attention 7

SI - System and Information Integrity

SI-2 Flaw Remediation

Status: Needs Attention

Requirement:

The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates;

d. Incorporates flaw remediation into the organizational configuration management process.

Outdated Assets (4 Assets):

asset0001	asset0002	asset0003	asset004

Vulnerabilities (18):

Flash Descriptor Unlocked (High - 7.5) **(4 Assets)**

asset0001	asset0002	asset0003	asset004

Microarchitectural Data Sampling (Medium - 6.5) (4 Assets)

asset0001	asset0002	asset0003	asset004

Outdated microcode (Medium - 5.0) (4 Assets)

asset0001	asset0002	asset0003	asset004

Spectre 3a: Rogue System Register Read (Medium - 4.3) (4 Assets)

asset0001	asset0002	asset0003	asset004

Intel ME Remote Privilege Escalation (Critical - 9.8) (4 Assets)

asset0001	asset0002	asset0003	asset004

Meltdown (Medium - 5.6) (4 Assets)

asset0001	asset0002	asset0003	asset004

SMI Unlocked (High - 8.2) (4 Assets)

asset0001	asset0002	asset0003	asset004

ROCA (Medium - 5.9) (4 Assets)

asset0001	asset0002	asset0003	asset004

DCI Debug Enabled (CVE-2017-5684) (Medium - 4.7) (4 Assets)

asset0001	asset0002	asset0003	asset004

Processor Memory Unlocked (High - 7.5) (4 Assets)

asset0001	asset0002	asset0003	asset004

Pantsdown (CVE-2019-6260). Aspeed BMC iLPC2AHB bridge misconfiguration (Critical - 9.8) (4 Assets)

asset0001	asset0002	asset0003	asset004

Flash Security Physically Disabled (High - 7.5) (4 Assets)

asset0001	asset0002	asset0003	asset004

Pantsdown (CVE-2019-6260). Aspeed BMC LPC2AHB bridge misconfiguration (Critical - 9.8) (4 Assets)

asset0001	asset0002	asset0003	asset004

Pantsdown (CVE-2019-6260). Aspeed BMC X-DMA engine misconfiguration (Critical - 9.8). (4 Assets)

asset0001	asset0002	asset0003	asset004

SI-3 Malicius Code Protection

Status: Needs Attention

Requirement:

The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:

1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy;

2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection;

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Outdated Assets (4):

asset0001 asset0002 asset0003 asset004

Vulnerabilities (19):

1. **Flash Descriptor Unlocked (High - 7.5) (4 Assets)**
   asset0001 asset0002 asset0003 asset004
2. **Insecure Flash Access Control (High - 7.5) (4 Assets)**
   asset0001 asset0002 asset0003 asset004
3. **Microarchitectural Data Sampling (Medium - 6.5) (4 Assets)**
   asset0001 asset0002 asset0003 asset004
4. **Spectre 4: Speculative Store Bypass (Medium - 4.3) (4 Assets)**
   asset0001 asset0002 asset0003 asset004
5. **Spectre 3a: Rogue System Register Read (Medium - 4.3) (4 Assets)**
   asset0001 asset0002 asset0003 asset004
6. **Spectre (OS Misconfiguration) (Medium - 5.6) (4 Assets)**
   asset0001 asset0002 asset0003 asset004
7. **Foreshadow (High - 7.3) (4 Assets)**
   asset0001 asset0002 asset0003 asset004
8. **Intel ME Remote Privilege Escalation (Critical - 9.8) (4 Assets)**
   asset0001 asset0002 asset0003 asset004
9. **Meltdown (Medium - 5.6) (4 Assets)**
   asset0001 asset0002 asset0003 asset004
10. **SMI Unlocked (High - 8.2) (4 Assets)**

asset0001 asset0002 asset0003 asset004

11. **ROCA (Medium - 5.9) (4 Assets)**

asset0001 asset0002 asset0003 asset004

12. **DCI Debug Enabled (CVE-2017-5684) (Medium - 4.7) (4 Assets)**

asset0001 asset0002 asset0003 asset004

13. **Processor Memory Unlocked (High - 7.5) (4 Assets)**

asset0001 asset0002 asset0003 asset004

14. **Pantsdown (CVE-2019-6260). Aspeed BMC iLPC2AHB bridge misconfiguration (Critical - 9.8) (4 Assets)**

asset0001 asset0002 asset0003 asset004

15. **Pantsdown (CVE-2019-6260). Aspeed BMC P2A Bridge misconfiguration (Critical - 9.8) (4 Assets)**

asset0001 asset0002 asset0003 asset004

16. **Flash Security Physically Disabled (High - 7.5) (4 Assets)**

asset0001 asset0002 asset0003 asset004

17. **Pantsdown (CVE-2019-6260). Aspeed BMC LPC2AHB bridge misconfiguration (Critical - 9.8) (4 Assets)**

asset0001 asset0002 asset0003 asset004

18. **Pantsdown (CVE-2019-6260). Aspeed BMC LPC2AHB bridge misconfiguration (Critical - 9.8) (4 Assets)**

asset0001 asset0002 asset0003 asset004

19. **Pantsdown (CVE-2019-6260). Aspeed BMC X-DMA engine misconfiguration (Critical - 9.8) (4 Assets)**

asset0001 asset0002 asset0003 asset004

Integrity Failures (73):

asset0001 asset0002 asset0003 asset004

Threats (17):

1. **Demo (4 Assets)**

asset0001 asset0002 asset0003 asset004

2. **smmbackdoor (4 Assets)**

asset0001 asset0002 asset0003 asset004

3. **lojax (4 Assets)**

asset0001 asset0002 asset0003 asset004

4. **pulsecureiocs (4 Assets)**

asset0001 asset0002 asset0003 asset004

5. **finspy (4 Assets)**

asset0001 asset0002 asset0003 asset004

6. ilobleed (4 Assets)

asset0001	asset0002	asset0003	asset004

7. genericfirewall (4 Assets)

asset0001	asset0002	asset0003	asset004

8. genericransomware (4 Assets)

asset0001	asset0002	asset0003	asset004

9. meris (4 Assets)

asset0001	asset0002	asset0003	asset004

10. blacklotus (4 Assets)

asset0001	asset0002	asset0003	asset004

11. ciscoiostalosimplant (4 Assets)

asset0001	asset0002	asset0003	asset004

12. cosmicstrand (4 Assets)

asset0001	asset0002	asset0003	asset004

13. ciscodeviceverification (4 Assets)

asset0001	asset0002	asset0003	asset004

14. ciscosecureboot (4 Assets)

asset0001	asset0002	asset0003	asset004

15. citrixadcwebshell (4 Assets)

asset0001	asset0002	asset0003	asset004

16. citrixbleed (4 Assets)

asset0001	asset0002	asset0003	asset004

17. sectionsioc (4 Assets)

asset0001	asset0002	asset0003	asset004

SI-4 Information System Monitoring

Status: Needs Attention

Requirement:

The organization:

a. Monitors the information system to detect:

1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives];

2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];

c. Deploys monitoring devices:

1. Strategically within the information system to collect organization-determined essential information;

2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

Missed Check-Ins (4):

asset0001 asset0002 asset0003 asset004

SI-7 Software, Firmware, and Information Integrity

Status: Needs Attention

Requirement:

Unauthorized modifications to boot firmware may be indicative of a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur, for example, if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the system component; and preventing unauthorized processes from modifying the boot firmware

Integrity Failures (4):

asset0001 asset0002 asset0003 asset004

SA - System And Services Acquisition

SA-22 Unsupported System Components

Status: Needs Attention

Requirement:

The organization:

a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer;

b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Outdated Assets (4):

asset0001 asset0002 asset0003 asset004

RA - Risk Assessment

RA-5 Vulnerability Scanning

Status: Needs Attention

Requirement:

a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;

2. Formatting checklists and test procedures;

3. Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;

e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Missed Check-Ins (4):

asset0001 asset0002 asset0003 asset004

MA - Maintenance Tools

MA-3 Maintenance Tools

Status: Needs Attention

Requirement:

The organization approves, controls, and monitors information system maintenance tools.

Supplemental Guidance

This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch.

Vulnerabilities (6):

1. **Pantsdown (CVE-2019-6260). Aspeed BMC iLPC2AHB bridge misconfiguration** (Critical - 9.8) **(4 Assets)**

   asset0001 asset0002 asset0003 asset004

2. **Pantsdown (CVE-2019-6260). Aspeed BMC LPC2AHB bridge misconfiguration** (Critical - 9.8) **(4 Assets)**

   asset0001 asset0002 asset0003 asset004

3. **Pantsdown (CVE-2019-6260). Aspeed BMC P2A Bridge misconfiguration** (Critical - 9.8) **(4 Assets)**

   asset0001 asset0002 asset0003 asset004

4. **Pantsdown (CVE-2019-6260). Aspeed BMC X-DMA engine misconfiguration (Critical - 9.8) (4 Assets)**

   asset0001 asset0002 asset0003 asset004

5. **Authentication Bypass in HPE iLO 4 (Critical - 9.8) (4 Assets)**

   asset0001 asset0002 asset0003 asset004

6. **Intel ME Remote Privilege Escalation (Critical - 9.8) (4 Assets)**

   asset0001 asset0002 asset0003 asset004

Appendix: Vulnerabilties

Flash Descriptor Unlocked

Severity: High - 7.5

Overview:
Flash Descriptor write-protection protects settings on the Flash from being maliciously or unintentionally changed after manufacturing is completed.

Description:
If the equipment manufacturer doesn't enable Intel-recommended Flash Descriptor write protections, a privileged, local attacker can modify the contents of the Flash Descriptor region. This allows an attacker to change access permissions for other regions or change layout for any regions which may be used to bypass hardware protections like PR registers and BIOS Control Register.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://github.com/abazhaniuk/Publications/blob/master/2017/44CON_2017/Bulygin_Bazhaniuk_44con.pdf

Insecure Flash Access Control

Severity: High - 7.5

Overview:

Flash Descriptor write-protection protects settings on the Flash from being maliciously or unintentionally changed after manufacturing is completed.

Description:
If the equipment manufacturer doesn't enable Intel-recommended Flash Descriptor write protections, a privileged, local attacker can modify the contents of the Flash Descriptor region. This allows an attacker to change access permissions for other regions or change layout for any regions which may be used to bypass hardware protections like PR registers and BIOS Control Register.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://github.com/abazhaniuk/Publications/blob/master/2017/44CON_2017/Bulygin_Bazhaniuk_44con.pdf

Microarchitectural Data Sampling

Severity: Medium - 6.5

Overview:
Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

Description:
Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. MDS is a sub-class of previously disclosed speculative execution side channel vulnerabilities and is comprised of four related techniques. Under certain conditions, MDS provides a program with the potential means to read data that the program otherwise would not be able to see. MDS techniques are based on a sampling of data leaked from small structures within the CPU using a locally executed speculative execution side channel. Practical exploitation of MDS is a very complex undertaking. MDS does not, by itself, provide an attacker with a way to choose the data that is leaked.

Recommendation:
We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html
https://software.intel.com/security-software-guidance/insights/deep-dive-intel-analysis-microarchitectural-datasampling

Outdated microcode

Severity: Medium - 5.0

Overview:
Latest microcode update is not installed on this system.

Description:
Microcode updates are used to mitigate vulnerabilities in the processor such as speculative execution sidechannel issues. This older microcode version may leave the system vulnerable to known attacks.

Recommendation:
We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:
https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/processorsaffected-consolidated-product-cpu-model.html

Spectre 3a: Rogue System Register Read

Severity: Medium - 4.3

Overview:
Common CPU hardware implementations are vulnerable to side-channel attacks known as Spectre and Meltdown.

Description:
Common CPU hardware implementations are vulnerable to side-channel attacks known as Spectre and Meltdown. Meltdown is a bug that "melts" the security boundaries normally enforced by the hardware, affecting desktops, laptops, and cloud computers. Spectre is a flaw that an attacker can exploit to force a CPU to reveal its data. Variant 3a is a vulnerability that may allow an attacker with local access to speculatively read system parameters via side-channel analysis and obtain sensitive information.

Recommendation:
We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html

Spectre (OS Misconfiguration)

Severity: Medium - 5.6

Overview:
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.

Description:
An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization). There are three primary variants of the issue which differ in the way the speculative execution can be exploited. Variant CVE-2017-5715 triggers the speculative execution by utilizing branch target injection. It relies on the presence of a precisely-defined instruction sequence in the privileged code as well as the fact that memory accesses may cause allocation into the microprocessor's data cache even for speculatively executed instructions that never actually commit (retire). As a

result, an unprivileged attacker could use this flaw to cross the syscall and guest/host boundaries and read privileged memory by conducting targeted cache side-channel attacks.

Recommendation:
We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2017-5715 https://access.redhat.com/security/cve/cve-2017-5715

Foreshadow

Severity: High - 7.3

Overview:
Also known as "Foreshadow" L1TF is a speculative execution attack on Intel processors which allows an attacker to steal sensitive information stored inside personal computers or third party clouds.

Description:
Also known as "Foreshadow" L1TF is a speculative execution attack on Intel processors which allows an attacker to steal sensitive information stored inside personal computers or third party clouds. Foreshadow has two versions, the original attack designed to extract data from SGX enclaves and a Next-Generation version which affects Virtual Machines (VMs), hypervisors (VMM), operating system (OS) kernel memory, and System Management Mode (SMM) memory.

Recommendation:
We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:
https://github.com/gregvish/l1tf-poc

Intel ME Remote Privilege Escalation

Severity: Critical - 9.8

Overview:
INTEL-SA-00075 is an escalation of privilege vulnerability in Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), and Intel Small Business Technology versions firmware versions 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5, and 11.6 that can allow an unprivileged attacker to gain control of the manageability features provided by these products. This vulnerability does not exist on Intel-based consumer PCs with consumer firmware, Intel servers utilizing Intel Server Platform Services (Intel SPS), or Intel Xeon Processor E3 and Intel Xeon Processor E5 workstations utilizing Intel SPS firmware.

Description:
There are two ways this vulnerability may be accessed. Please note that Intel Small Business Technology is not vulnerable to the first issue. - An unprivileged network attacker could gain system privileges to provisioned Intel manageability SKUs: Intel Active Management Technology (AMT) and Intel Standard Manageability (ISM) - An

unprivileged local attacker could provision manageability features gaining unprivileged network or local system privileges on Intel manageability SKUs: Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), and Intel Small Business Technology (SBT).

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00075.html

Meltdown

Severity: Medium - 5.6

Overview:
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.

Description:
An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization). There are three primary variants of the issue which differ in the way the speculative execution can be exploited. Variant CVE-2017-5754 relies on the fact that, on impacted microprocessors, during speculative execution of instruction permission faults, exception generation triggered by a faulting access is suppressed until the retirement of the whole instruction block. In a combination with the fact that memory accesses may populate the cache even when the block is being dropped and never committed (executed), an unprivileged local attacker could use this flaw to read privileged (kernel space) memory by conducting targeted cache side-channel attacks. Note: CVE-2017-5754 affects Intel x86-64 microprocessors. AMD x86-64 microprocessors are not affected by this issue.

Recommendation:
We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2017-5754 https://access.redhat.com/security/cve/cve-2017-5754

SMI Unlocked

Severity: High - 8.2

Overview:
Checks that the SMI events configuration is locked down

Description:
Global SMI Enable/SMI Lock - TCO SMI Enable/TCO Lock should be locked on the system. If it is not locked, in certain scenarios, this can be used by an attacker to compromise SMRAM and get full control over the system.

Recommendation:
Informational: Information to help evaluate the threat landscape / risks / threats.

Additional Information:
https://software.intel.com/sites/default/files/managed/85/7d/a_tour_beyond_bios_supporting_smm_resource_monitor_using_the_efi_developer_kit_ii.pdf
http://news.hitb.org/content/hitb2014kul-white-paper-using-intel-txt-attack-bioses

ROCA

Severity: Medium - 5.9

Overview:
ROCA vulnerability affecting RSA key generation in certain TPM implementations.

Description:
Some TPMs are affected by a vulnerability in the Infineon RSA library version 1.02.013, where they generate vulnerable RSA keys, as published in 2017. The keys generated by vulnerable components should not be considered secure. Note that ECC keys are not affected.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://crocs.fi.muni.cz/public/papers/rsa_ccs17 https://github.com/nsacyber/Detect-CVE-2017-15361-TPM
https://www.infineon.com/cms/en/product/promopages/tpm-update/?redirId=59160

DCI Debug Enabled (CVE-2017-5684)

Severity: Medium - 4.7

Overview:
Checks that the platform debug configuration is disabled and locked down

Description:
Platforms have debug mechanisms to assist in tracing back the source of faults, these mechanisms are sometimes used before a platform reaches production and sometimes it is used for refurbishing and fixing returned platforms. This module checks for CPU debug features and the Direct Connect Interface, both should be disabled and locked in a properly secure platform.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://conference.hitb.org/hitbsecconf2017ams/materials/D2T4%20-%20Maxim%20Goryachy%20and%20Mark%20Ermalov%20-%20Intel%20DCI%20Secrets.pdf

https://www.blackhat.com/docs/eu-17/materials/eu-17-Goryachy-How-To-Hack-A-Turned-Off-Computer-OrRunning-Unsigned-Code-In-Intel-Management-Engine.pdf

Processor Memory Unlocked

Severity: High - 7.5

Overview:
This is a verification that the memory map configuration is secure, checking if the memory map registers are correctly configured and locked down.

Description:
Some of the most important tasks a BIOS is in charge of are initialization of the platform hardware and properly report information to the underlying operating system. One of these configurations is the Memory map. The memory map should be properly configured, for example: registers, like TSEG, TOLUD should be locked. In case they are not locked, an attacker can use them to compromise firmware and get full control over the system.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://firmware.intel.com/sites/default/files/resources/A_Tour_Beyond_BIOS_Memory_Map_in%20UEFI_BIOS.pdf
https://www.slideshare.net/CanSecWest/csw2017-bazhaniuk-exploringyoursystemdeeperupdated

Pantsdown (CVE-2019-6260). Aspeed BMC iLPC2AHB bridge misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via LPC

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Pantsdown (CVE-2019-6260). Aspeed BMC P2A Bridge misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via PCI

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Flash Security Physically Disabled

Severity: High - 7.5

Overview:
Checks for SPI Controller Flash Descriptor Security Override Pin Strap (FDOPSS)

Description:
On some systems, this may be routed to a jumper on the motherboard and allows someone with physical access to the system to disable SPI memory protections. Possible attack scenario: jumper is hidden in pcb in design and from mfg phase allows this bypass to occur. Or it might be possible to downgrade ME and use these CVE's CVE2017-5705 CVE-2017-5706 CVE-2017-5707 CVE-2017-5708 CVE-2017-5709 CVE-2017-5710 CVE-2017-5711

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://ruxcon.org.au/assets/2016/slides/Firmware%20Biopsy.pdf https://reverse.put.as/2015/05/29/the-empire-strikes-back-apple-how-your-mac-firmware-security-is-completelybroken/

Pantsdown (CVE-2019-6260). Aspeed BMC LPC2AHB bridge misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via LPC

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Pantsdown (CVE-2019-6260). Aspeed BMC X-DMA engine misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via X-DMA engine

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services.

For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Flash Descriptor Unlocked

Severity: High - 7.5

Overview:
Flash Descriptor write-protection protects settings on the Flash from being maliciously or unintentionally changed after manufacturing is completed.

Description:
If the equipment manufacturer doesn't enable Intel-recommended Flash Descriptor write protections, a privileged, local attacker can modify the contents of the Flash Descriptor region. This allows an attacker to change access permissions for other regions or change layout for any regions which may be used to bypass hardware protections like PR registers and BIOS Control Register.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://github.com/abazhaniuk/Publications/blob/master/2017/44CON_2017/Bulygin_Bazhaniuk_44con.pdf

Insecure Flash Access Control

Severity: High - 7.5

Overview:
Flash Descriptor write-protection protects settings on the Flash from being maliciously or unintentionally changed after manufacturing is completed.

Description:
If the equipment manufacturer doesn't enable Intel-recommended Flash Descriptor write protections, a privileged, local attacker can modify the contents of the Flash Descriptor region. This allows an attacker to change access permissions for other regions or change layout for any regions which may be used to bypass hardware protections like PR registers and BIOS Control Register.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://github.com/abazhaniuk/Publications/blob/master/2017/44CON_2017/Bulygin_Bazhaniuk_44con.pdf

Microarchitectural Data Sampling

Severity: Medium - 6.5

Overview:

Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

Description:

Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. MDS is a sub-class of previously disclosed speculative execution side channel vulnerabilities and is comprised of four related techniques. Under certain conditions, MDS provides a program with the potential means to read data that the program otherwise would not be able to see. MDS techniques are based on a sampling of data leaked from small structures within the CPU using a locally executed speculative execution side channel. Practical exploitation of MDS is a very complex undertaking. MDS does not, by itself, provide an attacker with a way to choose the data that is leaked.

Recommendation:

We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html
https://software.intel.com/security-software-guidance/insights/deep-dive-intel-analysis-microarchitectural-datasampling

Spectre 4: Speculative Store Bypass

Severity: Medium - 4.3

Overview:

Common CPU hardware implementations are vulnerable to side-channel attacks known as Spectre and Meltdown.

Description:

Common CPU hardware implementations are vulnerable to side-channel attacks known as Spectre and Meltdown. Meltdown is a bug that "melts" the security boundaries normally enforced by the hardware, affecting desktops, laptops, and cloud computers. Spectre is a flaw that an attacker can exploit to force a CPU to reveal its data. Variant 5 is a vulnerability that exploits "speculative bypass". When exploited, Variant 4 could allow an attacker to read older memory values in a CPU's stack or other memory locations. While implementation is complex, this sidechannel vulnerability could allow less privileged code to read arbitrary privileged data and run older commands speculatively, resulting in cache allocations that could be used to exfiltrate data by standard side-channel methods.

Recommendation:

We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html

Spectre 3a: Rogue System Register Read

Severity: Medium - 4.3

Overview:
Common CPU hardware implementations are vulnerable to side-channel attacks known as Spectre and Meltdown.

Description:
Common CPU hardware implementations are vulnerable to side-channel attacks known as Spectre and Meltdown. Meltdown is a bug that "melts" the security boundaries normally enforced by the hardware, affecting desktops, laptops, and cloud computers. Spectre is a flaw that an attacker can exploit to force a CPU to reveal its data. Variant 3a is a vulnerability that may allow an attacker with local access to speculatively read system parameters via side-channel analysis and obtain sensitive information.

Recommendation:
We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html

Spectre (OS Misconfiguration)

Severity: Medium - 5.6

Overview:
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.

Description:
An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization). There are three primary variants of the issue which differ in the way the speculative execution can be exploited. Variant CVE-2017-5715 triggers the speculative execution by utilizing branch target injection. It relies on the presence of a precisely-defined instruction sequence in the privileged code as well as the fact that memory accesses may cause allocation into the microprocessor's data cache even for speculatively executed instructions that never actually commit (retire). As a result, an unprivileged attacker could use this flaw to cross the syscall and guest/host boundaries and read privileged memory by conducting targeted cache side-channel attacks.

Recommendation:
We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2017-5715 https://access.redhat.com/security/cve/cve-2017-5715

Foreshadow

Severity: High - 7.3

Overview:
Also known as "Foreshadow" L1TF is a speculative execution attack on Intel processors which allows an attacker to steal sensitive information stored inside personal computers or third party clouds.

Description:
Also known as "Foreshadow" L1TF is a speculative execution attack on Intel processors which allows an attacker to steal sensitive information stored inside personal computers or third party clouds. Foreshadow has two versions, the original attack designed to extract data from SGX enclaves and a Next-Generation version which affects Virtual Machines (VMs), hypervisors (VMM), operating system (OS) kernel memory, and System Management Mode (SMM) memory.

Recommendation:
We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:
https://github.com/gregvish/l1tf-poc

Intel ME Remote Privilege Escalation

Severity: Critical - 9.8

Overview:
INTEL-SA-00075 is an escalation of privilege vulnerability in Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), and Intel Small Business Technology versions firmware versions 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5, and 11.6 that can allow an unprivileged attacker to gain control of the manageability features provided by these products. This vulnerability does not exist on Intel-based consumer PCs with consumer firmware, Intel servers utilizing Intel Server Platform Services (Intel SPS), or Intel Xeon Processor E3 and Intel Xeon Processor E5 workstations utilizing Intel SPS firmware.

Description:
There are two ways this vulnerability may be accessed. Please note that Intel Small Business Technology is not vulnerable to the first issue. - An unprivileged network attacker could gain system privileges to provisioned Intel manageability SKUs: Intel Active Management Technology (AMT) and Intel Standard Manageability (ISM) - An unprivileged local attacker could provision manageability features gaining unprivileged network or local system privileges on Intel manageability SKUs: Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), and Intel Small Business Technology (SBT).

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00075.html

Meltdown

Severity: Medium - 5.6

Overview:
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.

Description:
An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization). There are three primary variants of the issue which differ in the way the speculative execution can be exploited. Variant CVE-2017-5754 relies on the fact that, on impacted microprocessors, during speculative execution of instruction permission faults, exception generation triggered by a faulting access is suppressed until the retirement of the whole instruction block. In a combination with the fact that memory accesses may populate the cache even when the block is being dropped and never committed (executed), an unprivileged local attacker could use this flaw to read privileged (kernel space) memory by conducting targeted cache side-channel attacks. Note: CVE-2017-5754 affects Intel x86-64 microprocessors. AMD x86-64 microprocessors are not affected by this issue.

Recommendation:
We are aware of a fix that should support this platform. Please install latest firmware updates from vendor advisory page.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2017-5754 https://access.redhat.com/security/cve/cve-2017-5754

SMI Unlocked

Severity: High - 8.2

Overview:
Checks that the SMI events configuration is locked down

Description:
Global SMI Enable/SMI Lock - TCO SMI Enable/TCO Lock should be locked on the system. If it is not locked, in certain scenarios, this can be used by an attacker to compromise SMRAM and get full control over the system.

Recommendation:
Informational: Information to help evaluate the threat landscape / risks / threats.

Additional Information:
https://software.intel.com/sites/default/files/managed/85/7d/a_tour_beyond_bios_supporting_smm_resource_monitor_using_the_efi_developer_kit_ii.pdf
http://news.hitb.org/content/hitb2014kul-white-paper-using-intel-txt-attack-bioses

ROCA

Severity: Medium - 5.9

Overview:
ROCA vulnerability affecting RSA key generation in certain TPM implementations.

Description:
Some TPMs are affected by a vulnerability in the Infineon RSA library version 1.02.013, where they generate vulnerable RSA keys, as published in 2017. The keys generated by vulnerable components should not be considered secure. Note that ECC keys are not affected.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://crocs.fi.muni.cz/public/papers/rsa_ccs17 https://github.com/nsacyber/Detect-CVE-2017-15361-TPM https://www.infineon.com/cms/en/product/promopages/tpm-update/?redirId=59160

DCI Debug Enabled (CVE-2017-5684)

Severity: Medium - 4.7

Overview:
Checks that the platform debug configuration is disabled and locked down

Description:
Platforms have debug mechanisms to assist in tracing back the source of faults, these mechanisms are sometimes used before a platform reaches production and sometimes it is used for refurbishing and fixing returned platforms. This module checks for CPU debug features and the Direct Connect Interface, both should be disabled and locked in a properly secure platform.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://conference.hitb.org/hitbsecconf2017ams/materials/D2T4%20-%20Maxim%20Goryachy%20and%20Mark%20Ermalov%20-%20Intel%20DCI%20Secrets.pdf https://www.blackhat.com/docs/eu-17/materials/eu-17-Goryachy-How-To-Hack-A-Turned-Off-Computer-OrRunning-Unsigned-Code-In-Intel-Management-Engine.pdf

Processor Memory Unlocked

Severity: High - 7.5

Overview:
This is a verification that the memory map configuration is secure, checking if the memory map registers are correctly configured and locked down.

Description:
Some of the most important tasks a BIOS is in charge of are initialization of the platform hardware and properly report information to the underlying operating system. One of these configurations is the Memory map. The memory map should be properly configured, for example: registers, like TSEG, TOLUD should be locked. In case they are not locked, an attacker can use them to compromise firmware and get full control over the system.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://firmware.intel.com/sites/default/files/resources/A_Tour_Beyond_BIOS_Memory_Map_in%20UEFI_BIOS.pdf
https://www.slideshare.net/CanSecWest/csw2017-bazhaniuk-exploringyoursystemdeeperupdated

Pantsdown (CVE-2019-6260). Aspeed BMC iLPC2AHB bridge misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via LPC

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Pantsdown (CVE-2019-6260). Aspeed BMC P2A Bridge misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via PCI

Description:

The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Flash Security Physically Disabled

Severity: High - 7.5

Overview:
Checks for SPI Controller Flash Descriptor Security Override Pin Strap (FDOPSS)

Description:
On some systems, this may be routed to a jumper on the motherboard and allows someone with physical access to the system to disable SPI memory protections. Possible attack scenario: jumper is hidden in pcb in design and from mfg phase allows this bypass to occur. Or it might be possible to downgrade ME and use these CVE's CVE2017-5705 CVE-2017-5706 CVE-2017-5707 CVE-2017-5708 CVE-2017-5709 CVE-2017-5710 CVE-2017-5711

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://ruxcon.org.au/assets/2016/slides/Firmware%20Biopsy.pdf https://reverse.put.as/2015/05/29/the-empire-strikes-back-apple-how-your-mac-firmware-security-is-completelybroken/

Pantsdown (CVE-2019-6260). Aspeed BMC LPC2AHB bridge misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via LPC

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access

is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Pantsdown (CVE-2019-6260). Aspeed BMC X-DMA engine misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via X-DMA engine

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Pantsdown (CVE-2019-6260). Aspeed BMC iLPC2AHB bridge misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via LPC

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Pantsdown (CVE-2019-6260). Aspeed BMC LPC2AHB bridge misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via LPC

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Pantsdown (CVE-2019-6260). Aspeed BMC P2A Bridge misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via PCI

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Pantsdown (CVE-2019-6260). Aspeed BMC X-DMA engine misconfiguration

Severity: Critical - 9.8

Overview:
Unauthenticated, arbitrary access to Baseboard Management Controller (BMC) from host via X-DMA engine

Description:
The ASPEED AST2400 and AST2500 Baseband Management Controller (BMC) hardware and firmware implement Advanced High-performance Bus (AHB) bridges, which allow arbitrary read and write access to the BMC's physical address space from the host. The typical consequence of external, unauthenticated, arbitrary AHB access is that the BMC fails to ensure all three of confidentiality, integrity and availability for its data and services. For instance it is possible to: reflash or dump the firmware of the BMC from the host, access BMC RAM, configure an in-band BMC console from the host, and disable the BMC until an AC power cycle.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://nvd.nist.gov/vuln/detail/CVE-2019-6260#vulnCurrentDescriptionTitle
https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260:-gaining-control-of-bmc-from-the-host-processor/

Authentication Bypass in HPE iLO 4

Severity: Critical - 9.8

Overview:
Remote authentication bypass and code execution vulnerability in iLo 4

Description:
HPE iLo 4, versions prior to 2.53 contain vulnerabilities that could allow an attacker to bypass authentication and obtain remote code execution. Affected systems should be updated to the latest firmware in order to mitigate this issue.

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03769en_us

Intel ME Remote Privilege Escalation

Severity: Critical - 9.8

Overview:
INTEL-SA-00075 is an escalation of privilege vulnerability in Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), and Intel Small Business Technology versions firmware versions 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5, and 11.6 that can allow an unprivileged attacker to gain control of the manageability features provided by these products. This vulnerability does not exist on Intel-based consumer PCs with consumer firmware, Intel servers utilizing Intel Server Platform Services (Intel SPS), or Intel Xeon Processor E3 and Intel Xeon Processor E5 workstations utilizing Intel SPS firmware.

Description:
There are two ways this vulnerability may be accessed. Please note that Intel Small Business Technology is not vulnerable to the first issue. - An unprivileged network attacker could gain system privileges to provisioned Intel manageability SKUs: Intel Active Management Technology (AMT) and Intel Standard Manageability (ISM) - An unprivileged local attacker could provision manageability features gaining unprivileged network or local system privileges on Intel manageability SKUs: Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), and Intel Small Business Technology (SBT).

Recommendation:
Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00075.html