The Intel® Converged Security Management Engine (CSME) Delayed Authentication Mode (DAM) vulnerability - CVE-2018-3659 and CVE-2018-3643

White paper

Revision 1.0
June 2020

Legal Disclaimer

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

The products described might contain design defects or errors known as errata, which might cause the product to deviate from published specifications. Current, characterized errata are available on request.

Intel technologies might require enabled hardware, software, or service activation. Some results have been estimated or simulated. Your costs and results might vary.

No product or component can be absolutely secure.

Purpose of the white paper

The purpose of this white paper is to provide technical details to help understand the Intel® Converged Security Management Engine (CSME) Delayed Authentication Mode (DAM) issue (CVE-2018-3659 and CVE-2018-3643), how it could be potentially exploited, and the resulting impact of a successful exploitation.

The white paper also discusses the CSME Firmware mitigations made to help prevent exploitation of CVE-2018-3659 and CVE-2018-3643 and what steps are recommended to protect systems against potential attacks.

While most of the technical information contained in this white paper was already documented publicly as part of a Black Hat presentation on CSME in August 2019, the intent of the white paper is to augment that information further in light of recent, public disclosures regarding the security of the CSME on certain Intel products.

Contents

Purpose of the white paper 3

Background 5

The vulnerability 7

The CVE mitigations 9

Hardware based Anti-rollback (ARB) 10

The impact of the CVE 10

Use Case support per SoC / PCH 12

How DAM can be triggered? 12

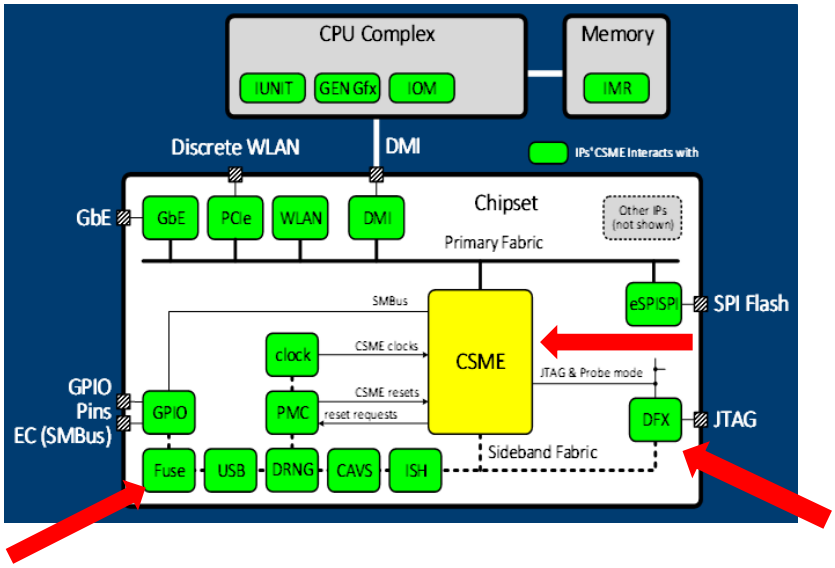
Impact of CVE per of Client/Server system 13

Note on CVE description 14

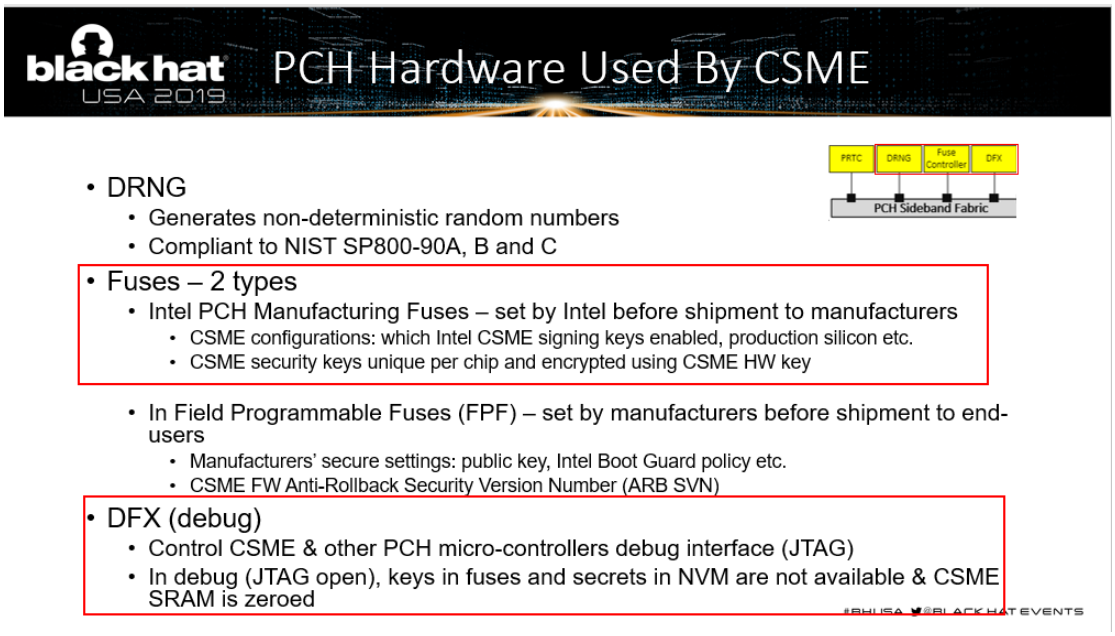
Background

The Intel Platform Controller Hub (PCH)/System on Chip (SoC) consists of a set of hardware blocks (aka IP or IPs) connected by an internal fabric as illustrated in figure hereafter. The Intel CSME is one of those hardware blocks.

It is important to note that this figure is for illustrative purposes only and does not reflect the exact hardware block diagram for PCH and SoC products.



This document focuses on the interactions between CSME, DFX (Design for Testability, Debug, Security and Validation) and the Fuse (aka fuse controller).



The DFX IP is responsible to indicate the debug policy to other IPs within the PCH / SoC like CSME and Fuses. Once the DFX policy is changed, IPs are notified and responsible to scrub any secrets that may be present inside the IP before they open their debug interfaces.

For example, CSME scrubs its secrets (i.e. Fuse Encryption Key, Digital Right Management and Trusted Platform Module keys, storage keys, chipset key and Intel® Enhanced Privacy ID (EPID) private key) from Hardware (e.g. Secure Key Storage, internal buses etc.) and internal memory (aka CSME SRAM) before it opens its debug interface (JTAG). In addition, CSME chipset key and EPID key kept in fuses are blocked by fuse controller when DFX policy is changed and the only key available in this case is the debug-enabled chipset key. The table below lists the CSME keys programmed by Intel into the PCH/SOC fuses.

CSME Security Fuses	Length in bit	Encrypted with Fuse Encryption Key	Available on debug
Chipset Key	256	Yes	No
Intel® Platform Trust Technology (PTT) EK Counters	32	No	Yes
EPID 1.0 Group ID	32	No	Yes
EPID 1.0 Private Key	256	Yes	No
EPID 2.0 Group ID*	32	No	Yes
EPID 2.0 Private Key*	256	Yes	No
Debug Enabled Chipset Key	128	No	Yes

*Present only starting Cannon Point (CNP) PCH

The CSME Hardware scrubbing and the fuse controller blocking the CSME chipset key and EPID private keys are done in order to help ensure that even authorized Intel or system manufacturer personnel won't be exposed to CSME secrets.

CSME Firmware is responsible to verify debug token, if present in UTOK partition of CSME region in SPI flash. These debug tokens can be either signed by Intel or the system manufacturer and are specific to the system (bound to the PCH/SoC ID). Once the debug token has been verified, the CSME Firmware will request from the CSME ROM to change the DFX policy in DFX aggregator.

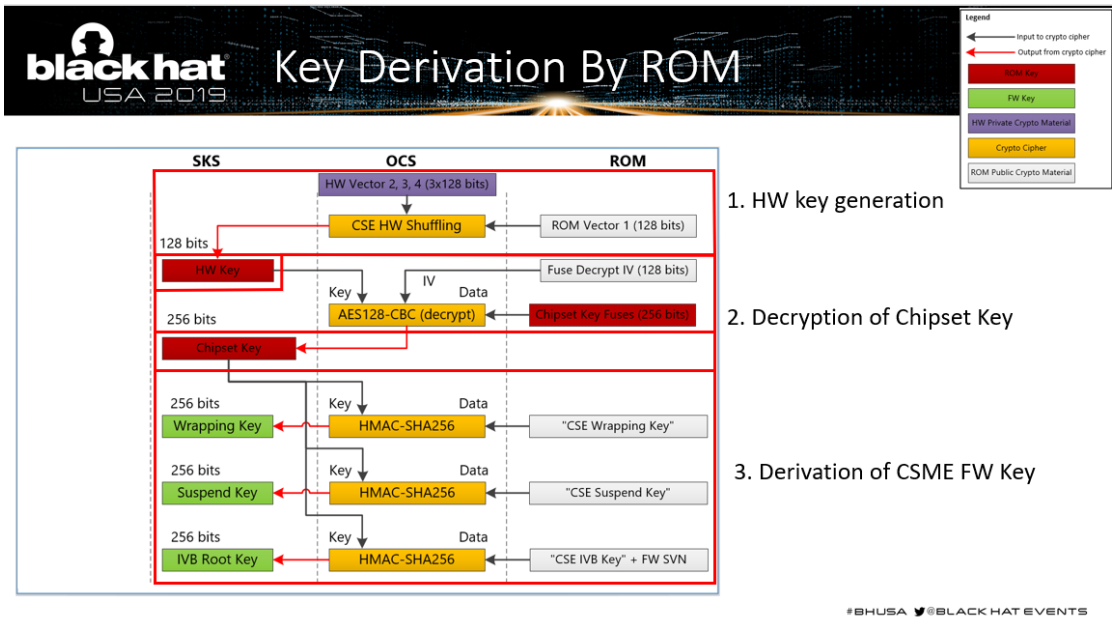
There are four main levels of DFX policy as indicated in table below.

DFX Policy	CSME keys in fuses	CSME Debug interface	Authorization level	Comments
Green	Available	Closed	N/A	It is the normal fully functional state of the chip, aka DFX locked state
Orange	Unavailable	Closed*	System Manufacturer	It is the state allowing to debug IPs that can be customized by system manufacturer. CSME secrets are not available.
Red	Unavailable	Opened	Intel	It is the state allowing Intel to debug any IP in PCH/SoC. CSME secrets are not available.
DAM	Unavailable	Closed	None	It is a special state where the system is prepared for debugging (i.e. CSME secrets are cleared), but the debug interfaces are still closed. CSME secrets are not available.

* On Broxton-P and Geminilake SoC, CSME Debug interface is opened

CVE-2018-3659 and CVE-2018-3643 vulnerabilities

When PCH/SoC DFX policy is set to DAM, the CSME ROM only gets the debug enabled chipset key from fuse controller and uses a zeroed encrypted chipset key (also referenced as “zeroed chipset key” in later section of the white paper) instead of the real chipset key encrypted with the Fuse Encryption Key (denoted as chipset key fuses in diagram below). In addition, CSME Hardware scrubs the real Fuse Encryption Key (denoted as HW key in diagram below). Therefore, when ROM decrypts the zeroed encrypted chipset key, it is done with a zeroed Fuse Encryption Key and the Fuse IV hard coded in CSME ROM (denoted as Fuse Decrypt IV in diagram below).



Once the Fuse IV is successfully extracted from the CSME ROM (e.g. by exploiting CVE-2019-0090), the chipset and all subsequent keys derived from it by CSME ROM and Firmware can be easily discovered when platform is not in DFX locked state. In addition, the keys would be identical across all systems having same PCH or SoC generation.

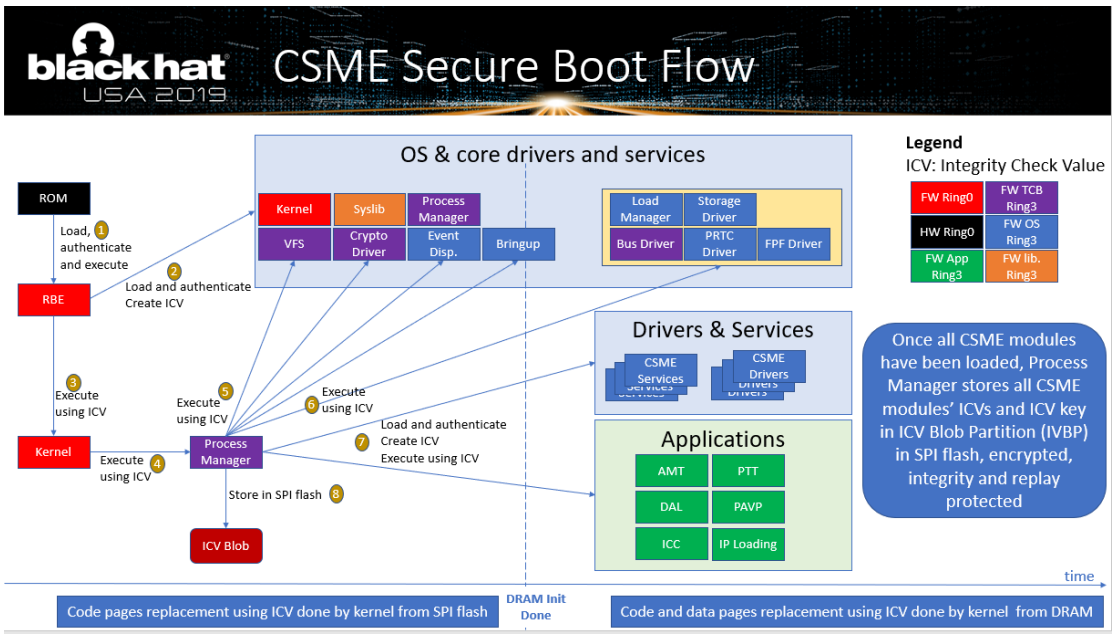
It is still important to note that the real CSME chipset key and EPID private key are scrubbed, and so this attack does not compromise them or use cases relying on them (i.e. remote attestation for HW DRM). Also, any secret kept in SPI flash and protected by CSME storage keys when system is in DFX lock state, can’t be read by CSME Firmware when DFX policy changes.

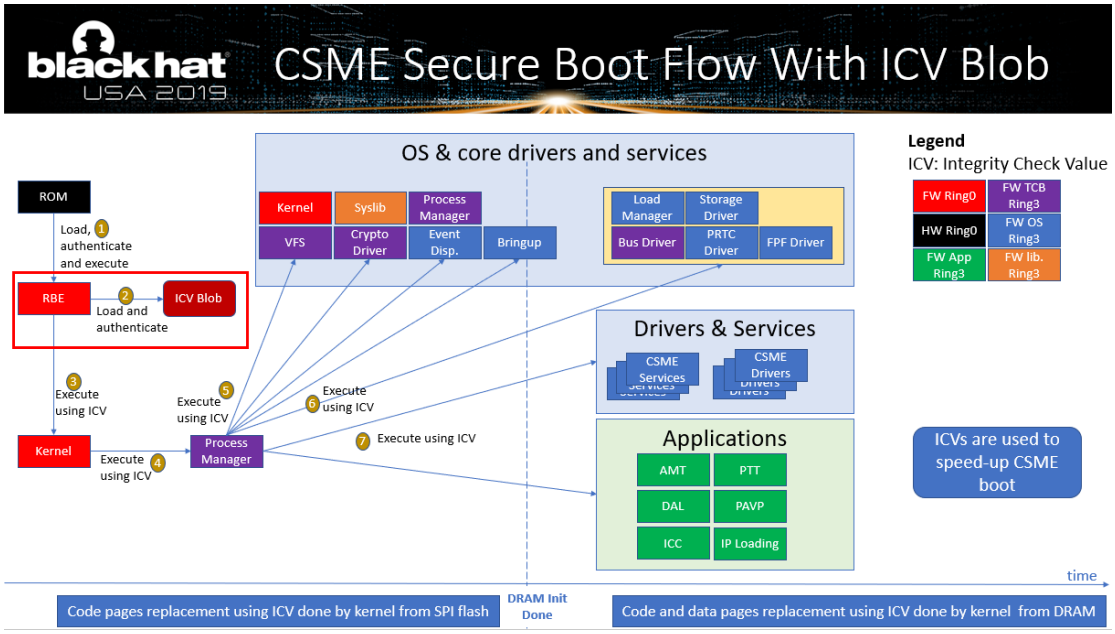
In addition, changing the DFX policy to DAM does not require Intel or system manufacturer authorization (in the form of a signed debug token) and can be set through physical or local access with user consent.

Combining “zeroed chipset key” and lack of authorization to enable DAM, it may allow an attacker with physical access to a system to enable DAM and know the CSME keys generated by CSME ROM and Firmware.

Some of these keys are essential to CSME Firmware execution integrity and protect CSME data kept in SPI flash (e.g. Intel PTT data):

- Intel Root Key – this key is the master key for the CSME firmware. For example, it is used to generate storage keys that would protect CSME data in SPI flash (aka Non-Volatile Memory:(NVM)).
- IVB Root Key – this key is used to help protect the Integrity Protection Key (IPK) and the CSME Firmware modules' Integrity Check Value (ICVs calculated using IPK and Crypto Hardware accelerator AES-Paging engine over CSME Firmware module's 4KB pages) in NVM. The ICVs allow faster boot of CSME Firmware and to securely page out and page in CSME code and data from CSME SRAM to SPI flash/DRAM. IPK and ICV are invalidated upon CSME Firmware update or an ICV integrity failure. This key is critical to CSME execution integrity during boot and runtime as shown in below diagrams for CNP based platform.





Furthermore, when system is in DAM, the CSME Intel Root Key and IVB Root Key would be constant across all systems sharing same PCH or SoC generation, and once discovered can be used on all those systems. This type of attack is commonly known as a Break One Run Everywhere (BORE) attack.

CVE-2018-3659 and CVE-2018-3643 mitigations

Intel has provided a mitigation to the CVEs as follows:

1. 1. The CSME ROM Boot Extension (RBE) Firmware module regenerates all Firmware root keys and IVB root key from the “Non-Intel” Root Key (previously derived by ROM using the debug enabled chipset key) when RBE detects that the DFX policy is not in lock state. As explained above, the debug enabled chipset key is the only key available in this DFX state, it has the property to have high entropy and to be unique per PCH/SoC.
2. The Intel PTT enters failure mode when it fails to read its NVM data due to DFX policy change. That’s because, the CSME storage keys used to protect PTT NVM data in DFX locked state are different from the storage keys when in DFX unlocked or DAM state.

The latest CSME Firmware includes mitigations for the DAM issue against known attacks. When Hardware-based Anti-rollback (ARB) capability is supported and enabled by system manufacturer (including BIOS support), the CSME will only accept the latest CSME Firmware, mitigating against physical firmware rollback attacks.

In addition, as specified in Intel guidelines to system manufacturers, End-Of-Manufacturing (EOM) should be applied by system manufacturer before shipment. EOM provides the following controls:

1. SPI descriptor, containing access control list on different region (i.e., BIOS, CSME), is locked and cannot be changed by locally executing Software. The access control is then enforced by the SPI controller.

2. SPI Flash-based fuse emulation is disabled and Field Programmable Fuses in PCH or SoC are used instead.
3. CSME Manufacturing APIs are disabled.

Hardware based Anti-rollback (ARB)

In order to mitigate physical attack vectors, the CSME Hardware-based, Anti-rollback capability (ARB) must be supported by the PCH/SoC and enabled by the system manufacturers. This capability will prevent a physical roll back of the CSME Firmware in flash and provide resilience that the system is less likely being exploited by known vulnerabilities that have been mitigated in the most recently released CSME Firmware updates.

This table summarizes in which PCH/SoC and under which conditions Hardware-based ARB is supported.

	PCH / SOC							
	BXT-P	GLK	SPT	KBP	LBG	DNV	DNV-AD	CNP
Hardware based ARB supported	Yes	Yes	No	No	No	No	Yes	Yes
Required enablement during system manufacturing by manufacturers	Yes	Yes	N/A	N/A	N/A	N/A	Yes	No
Required support in manufacturers BIOS	Yes	Yes	N/A	N/A	N/A	N/A	Yes	Yes

The impact of the vulnerability

The vulnerability may allow an attacker to load their own CSME Kernel Firmware module and compromise some of the CSME use-cases on the system.

The table hereafter lists the different use cases supported by CSME and how they could be potentially impacted by the vulnerability

Use case	Description	Potential Consequence
Silicon Enabling	Base initialization of PCH/SoC including clocks and GPIOs	Denial of service.
Intel Boot Guard	Authenticate BIOS - prevents software update and simple physical attack to install unauthorized BIOS	Unauthorized BIOS compromises OS loader and OS integrity.
Intel Platform Trust Technology (PTT) – Integrated TPM 2.0	Integrated TPM to support UEFI secure boot, disk encryption, virtual smart card, remote attestation	Intel PTT may store TPM keys (e.g. disk encryption key) in SPI flash protected by known CSME storage keys when switching to DAM DFX policy Note there is no consequences for following use cases: 1. Remote attestation use cases relying on Endorsement Key (EK) are not impacted. Intel PTT uses

		a debug EK when not in DFX locked state 2. PTT keys protected by CSME Firmware in SPI flash while system was in DFX lock state are not available when switching to another DFX policy (i.e. DAM)
Protected Audio Video Path (PAVP) / Digital Rights Management (DRM) on client platform only	Hardware-based DRM, HDCP link protection	No consequences because 1. The content provider will be able to detect that the firmware is working with the test key DRM keys protected by CSME Firmware in SPI flash while system was in DFX lock state are not exposed when switching to another DFX policy (i.e. DAM)
Intel Active Management Technology (AMT) on client platform only	Remote management, assistance, recovery, of enterprise PCs	Compromise boot, and OS integrity using AMT. Note that corporate secrets stored on AMT in SPI flash while system was in DFX lock state are not exposed when switching to another DFX policy (i.e. DAM)
Intel Dynamic Application Loader (DAL) on client platform only	Secure loading and execution of Intel signed DAL applet like Intel® Authenticate, Intel Identity Protection Technology, Intel® Software Guard Extensions (SGX) Time and Monotonic Counter Services (for SGX DRMs), and more.	Loading of unsigned DAL applet Note that Intel use cases relying on SIGMA/EPID are not impacted. They can still be trusted because the CSME EPID private key is not available when system is not in DFX lock state.
Firmware Authentication for IPs	Secure loading of Power Management Controller, Integrated Sensor Hub, Audio DSP, Image Processing Unit (IPU) Firmware	Unauthorized control of these IPs
PCH/SoC Debug	Authorize and configure debug policies that can unlock the PCH / SoC in various modes (Green, Orange, Red)	Unauthorized reverse engineering and debug of Intel and OEM intellectual property
Intel Node Manager on server platform only	Platform-level, power management and telemetry	Platform power policies configured by the administrator are not obeyed. Telemetry data are not trusted.

It is important to note that the following Intel CPU-based security technologies are not impacted by DAM CVE:

1. Intel® Trusted Execution Technology (TXT), if used with a discrete TPM and not Intel PTT. TXT in this white paper refers to Intel CPU Dynamic Root of Trust for Measurement (DRTM) that establishes a new Trusted Computing Base (TCB) starting from the CPU micro-code and not a specific TXT usage by a specific Measured Launched Environment (MLE) or Virtual Machine Manager (VMM).
2. Intel SGX including the secure time and monotonic counter services on client platform only that are provided by CSME DAL and secured by Intel SIGMA/EPID
3. Intel® Virtualization Technology for Directed I/O (VT-d) - proper configuration of Intel VT-d prevents rogue DMA access to system memory by a compromised CSME because such memory access is conforming to Peripheral Component Interconnect (PCI) memory transactions which include CSME devices' PCI Bus/Device/Function(BDFs) that can be managed by VT-d.

Use Case support per SoC / PCH

The table below lists which use case is supported on which SoC / PCH:

Use Case	PCH / SoC							
	BXT-P	**GLK**	**SPT**	**KBP**	**LBG**	**DNV**	**DNV-AD**	**CNP**
Silicon Enabling	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel Boot Guard	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Intel Platform Trust Technology	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Hardware DRM	Yes	Yes	Yes	Yes	No	No	No	Yes
Intel Active Management Technology	No	No	Yes	Yes	Yes[2]	No	No	Yes[2]
Intel Dynamic Application Loader	Yes	Yes	Yes	Yes	Yes[2]	No	No	Yes[2]
Firmware Authentication for IPs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PCH/SoC Debug	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel Node Manager	No	No	Yes[3]	No	Yes[3]	Yes[1]	No	No
Hardware "health" check	No	No	No	No	No	No	Yes	No

Yes[1] – Intel Node Manager functionality provides telemetry only, no system power management.

Yes[2] – Use case is supported only on Workstations systems that run CSME Firmware. On Server (Intel® Server Platform Services Firmware), the use case is not supported.

Yes[3] – Use case is supported only on Server that runs SPS Firmware. On Workstation or Client (CSME Firmware), the use case is not supported.

The "Firmware authentication for IP" use case might also differ between client and server. For example, even though Integrated sensor hub (ISH) Hardware exists in CNP-H PCH used on server platform, SPS Firmware does not support loading of ISH Firmware.

How DAM can be triggered?

As already stated above, DAM doesn't require Intel or system manufacturer authorization; however, it does require user consent for privacy reasons, to ensure system can't be debugged without user's knowledge.

The consent can be set in the following way:

- On CNP based platform, by physically connecting to Intel® Direct Connect Interface (Intel® DCI) over a USB3 port supporting a dedicated protocol and device for debugging, aka Intel® DCI OOB.
- Having BIOS set consent.
- Setting DCI enable bit in SPI descriptor, i.e. a configuration option that enable/disable automatic debug consent if the system is before EOM. This can be set using Intel Flash Image Tool (FIT).

Impact of vulnerability per of Client/Server system

This table lists client systems for CSME and Intel® Converged Security Engine (CSE):

CSME & CSE Version	PCH/SOC	Platform code name	CVE-2018-3659	CVE-2018-3643
CSME 15	TGP	Tigerlake	Not affected	Not affected
CSME 13.30	LKF	Lakefield	Not affected	Not affected
CSE 13.50	JSL-N	Jasperlake	Not affected	Not affected
CSME 14.5	CMP-V	Cometlake-V	Not affected	Not affected
CSME 14	CMP	Cometlake	Not affected	Not affected
CSME 13	ICP	Icelake	Not affected	Not affected
CSME 12	CNP	Cannonlake Coffeelake Whiskeylake Mehlow Workstation	Affected	Affected
CSE 4	GLK	Geminilake	Affected	Affected
CSE 3	BXT-P	Apollolake Gordon Peak	Affected	Affected
CSME 11	SPT KBP LBG	Skylake & Amberlake Kabylake & Basin/Glacier Falls Purley Workstation	Not affected*	Not affected*

*DAM is not supported on those platform

This table lists server systems Intel® Server Platform Services (SPS) Firmware or Intel® Advanced Driver Assistance Systems (ADAS) Management Engine Firmware

SPS / ADAS Version	PCH/SOC	Platform code name	CVE-2018-3659	CVE-2018-3643
SPS E3_06.00	TGP-H	Tatlow	Not affected	Not affected
SPS E5_06.00	EBG	Eaglestream	Not affected	Not affected
SPS SoC-X_05.00	CDF	Idaville	Not affected	Not affected
SPS SoC-A_05.00	CDF	Jacobsville	Not affected	Not affected
SPS E3_05.00 **SPS E3_05.01**	CNP-H	Mehlow Mehlow Refresh	Affected	Affected
SPS E5_04.04	LBG-R	Whitley	Not affected	Not affected

ADAS_ME_54	DNV-AD	Carlake	Not affected*	Not affected*
SPS SoC-X_04.00	SPT-D	Bakerville	Not affected*	Not affected*
SPS SoC-A_04.00	DNV	Harrisonville	Not affected*	Not affected*
SPS E3_04.00 **SPS E3_04.01** **SPS E3_04.08**	SPT-H	Greenlow Greenlow Refresh Montevista	Not affected*	Not affected*
SPS E5_04.00 **SPS E5_04.01**	LBG	Purley Purley Refresh	Not affected*	Not affected*

*DAM is not supported on those platform

Note on CVE-2018-3659 and CVE-2018-3643 description

CVEs description does not mention DAM explicitly. Furthermore, the description of impact is spread across 2 CVEs. The first CVE describes the Intel PTT impact, and the later CVE describes the potential for arbitrary code execution inside CSME.