SECURITY INFORMATION SUMMARY

SECURITY VULNERABILITIES CONCERNING DYNABOOK PC PRODUCTS

- THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.
- "INTEL" IS A TRADEMARK OF INTEL CORPORATION IN THE U.S. AND OTHER COUNTRIES.
- OTHER NAMES AND BRANDS MAY BE CLAIMED AS THE PROPERTY OF OTHERS.

Last modified: September 16, 2020

CHANGE HISTORY

dynabook

1

DATE	VENDOR ID	VULNERABILITY DESCRIPTION
Sep 16, 2020	Intel-SA-00337	Intel® Wireless Bluetooth® Advisory
	Intel-SA-00355	Intel® PROSet/Wireless WiFi Software Advisory
Aug 05, 2020	Intel-SA-00366	Intel® Innovation Engine Advisory
Jul 21, 2020	Intel-SA-00322	2020.1 IPU - BIOS Advisory2020.1 IPU - BIOS Advisory
	Intel-SA-00320	Special Register Buffer Data Sampling Advisory
	Intel-SA-00295	2020.1 IPU – Intel® CSME, SPS, TXE, AMT, ISM and DAL Advisory
Apr 15, 2020	Intel-SA-00338	Intel® PROSet/Wireless WiFi Software Advisory
Mar 30, 2020	Intel-SA-00330	Intel® Snoop Assisted L1D Sampling Advisory
Mar 26, 2020	Intel-SA-00315	Intel® Processor Graphics Advisory
	Intel-SA-00326	Intel® Optane™ DC Persistent Memory Module Management Software Advisory
	Intel-SA-00334	Intel® Processors Load Value Injection Advisory
Mar 02, 2020	Intel-SA-00329	Intel® Processor Data Leakage Advisory
	Intel-SA-00314	Intel® Processor Graphics Advisory
Feb 24, 2020	Intel-SA-00307	Intel® CSME Advisory
Dec 18, 2019	Intel-SA-00324	Intel® RST Advisory
	Intel-SA-00317	Unexpected Page Fault in Virtualized Environment Advisory
	Intel-SA-00289	Intel® Processors Voltage Settings Modification Advisory
	Intel-SA-00270	2019.2 IPU – TSX Asynchronous Abort Advisory
	Intel-SA-00260	Intel® Processor Graphics 2019.2 IPU Advisory
	Intel SA-00253	Intel® Ethernet I218 Adapter Driver for Windows Advisory
	Intel-SA-00241	Intel® CSME, Intel® SPS, Intel® TXE, Intel® AMT, Intel® PTT and Intel® DAL Advisory
	Intel-SA-00220	Intel® SGX and Intel® TXT Advisory

CHANGE HISTORY

2

DATE	VENDOR ID	VULNERABILITY DESCRIPTION
May 14, 2019	Intel-SA-00233	Micro architectural Data Sampling Advisory
May 14, 2019	Intel-SA-00213	Intel® CSME, Intel® SPS, Intel® TXE, Intel® DAL, and Intel® AMT 2019.1 QSR Advisory
Mar 03, 2019	Intel-SA-00191	Intel® Firmware 2018.4 QSR Advisory
Mar 03, 2019	Intel-SA-00189	Intel® Graphics Driver for Windows* 2018.4 QSR Advisory
Mar 03, 2019	Intel-SA-00185	Intel® CSME, Server Platform Services, Trusted Execution Engine and Intel® Active Management Technology 2018.4 QSR Advisory
Jan 08, 2019	Intel-SA-00182	Intel® PROSet/Wireless WiFi Software Advisory
Sep 11, 2018	Intel-SA-00142	Intel® Platform Trust Technology (PTT) Update Advisory
Sep 11, 2018	Intel-SA-00141	Intel® Active Management Technology 9.x/10.x/11.x/12.x Security Review Cumulative Update Advisory
Sep 11, 2018	Intel-SA-00125	Intel® CSME Assets Advisory
Aug 14, 2018	Intel-SA-00161	Q3 2018 Speculative Execution Side Channel Update
July 09, 2018	Intel-SA-00118 Intel-SA-00112	Intel® AMT 9.x/10.x/11.x Security Review Cumulative Update & Intel® ME 11.x issue
Jan 03, 2018	Intel-SA-00088	Intel® Processor firmware vulnerability
May 21, 2018	Intel-SA-00115	Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method
Apr 03, 2018	Intel-SA-00087	Unsafe Opcodes exposed in Intel® SPI based products
Jan 31, 2018	Intel-SA-00089	Intel® Graphics Drivers for Windows Code can fail to adequately validate a pointer input
Dec 12, 2017	Intel-SA-00095	Intel® Content Protection HECI Service has a Type Confusion vulnerability which potentially can lead to a privilege escalation
Oct 10, 2017		Potential vulnerability in Infineon® TPM (Trusted Platform Module) used in Dynabook Inc. notebook products
Nov 20, 2017	Intel-SA-00082 Intel-SA-00086	Intel AMT® Upgradable to Vulnerable Firmware, Intel® Security Vulnerabilities Regarding Intel® Management Engine (ME), Intel® Server Platform Services (SPS), and Intel® Trusted Execution Engine (TXE)
Oct 16, 2017	Intel-SA-00101	One or more Intel® Products affected by the Wi-Fi Protected Access II (WPA2) protocol vulnerability
May 01, 2017	Intel-SA-00075	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
Jan 12, 2018		Intel® AMT password security issue (F-Secure)

Intel® Wireless Bluetooth® Advisory (Intel-SA-00337)

INTRODUCTION

Intel® Wireless Bluetooth® Advisory

VULNERABILTY SUMMARY

INTEL-SA-00337

- Potential security vulnerabilities in some Intel® Wireless Bluetooth® products may allow denial of service, information disclosure or escalation of privilege. Intel is releasing firmware and software updates to mitigate these potential vulnerabilities.
- Vulnerability Details:

  CVEID: **CVE-2020-0554 /** CVEID: **CVE-2020-0555 /** CVEID: **CVE-2020-0553 /** CVEID: **CVE-2019-14620**

- Affected Products:

  Intel® Wireless Bluetooth® products:

  Intel® Wi-Fi 6 AX201, Intel® Wi-Fi 6 AX200, Intel® Wireless-AC 9560, Intel® Wireless-AC 9462, Intel® Wireless-AC 9461, Intel® Wireless-AC 9260, Intel® Dual Band Wireless-AC 8265, Intel® Dual Band Wireless-AC 8260, Intel® Dual Band Wireless-AC 3168, Intel® Wireless 7265 (Rev D) Family, Intel® Dual Band Wireless-AC 3165

- **Intel® security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00337.html

STATUS

- **RESOLVED**

RESOLUTION

Dynabook Inc. continues to work with Intel® on updates with new versions available per guidance from Intel's Security Issue Update.

To download the latest Intel® Wireless Bluetooth® driver (Version 21.90.0.4 / TCH0765100A) published by Dynabook Inc., please visit http://emea.dynabook.com/support/drivers/laptops/.

Intel® PROSet/Wireless WiFi Software Advisory (Intel-SA-00355)

INTRODUCTION

Intel® PROSet/Wireless WiFi Software Advisory

VULNERABILTY SUMMARY

INTEL-SA-00355

- A potential security vulnerability in some Intel® PROSet/Wireless WiFi products may allow escalation of privilege. Intel is releasing software updates to mitigate this potential vulnerability.
- Vulnerability Details:

  CVEID: **CVE-2020-0559**

- Affected Products:

  Intel® Wireless Bluetooth® products:

  Intel® Wi-Fi 6 AX201, Intel® Wi-Fi 6 AX200, Intel® Wireless-AC 9560, Intel® Wireless-AC 9462, Intel® Wireless-AC 9461, Intel® Wireless-AC 9260, Intel® Dual Band Wireless-AC 8265, Intel® Dual Band Wireless-AC 8260, Intel® Dual Band Wireless-AC 3168, Intel® Wireless 7265 (Rev D) Family, Intel® Dual Band Wireless-AC 3165

- **Intel® security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00355.html

STATUS

- **RESOLVED**

RESOLUTION

Dynabook Inc. continues to work with Intel® on updates with new versions available per guidance from Intel's Security Issue Update.

To download the latest Intel® Wireless LAN driver (Version 21.90.3.2 / TCH0771800A) published by Dynabook Inc., please visit http://emea.dynabook.com/support/drivers/laptops/.

Intel® Innovation Engine Advisory (Intel-SA-00366)

INTRODUCTION

Intel® Innovation Engine Advisory

VULNERABILTY SUMMARY

INTEL-SA-00366

- A potential security vulnerability in the Intel® Innovation Engine Build and Signing Tool may allow escalation of privilege. Intel is releasing software updates to mitigate this potential vulnerability.
- Vulnerability Details:

  CVEID: **CVE-2020-8675**
  Description: Insufficient control flow management in firmware build and signing tool for Intel® Innovation Engine before version 1.0.859 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.

- Affected Products:

  Intel® Innovation Engine Build and Signing Tool before version 1.0.859.

- **Intel® security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00366.html

STATUS

- **UNDER REVIEW**

RESOLUTION

Dynabook Inc. continues to work with Intel® on updates with new versions available per guidance from Intel's Security Issue Update.

As soon as Dynabook Inc. finalized examination of this vulnerability, we will share more information.

INTRODUCTION

2020.1 IPU - BIOS Advisory2020.1 IPU - BIOS Advisory

VULNERABILTY SUMMARY

INTEL-SA-00322

- Potential security vulnerabilities in BIOS firmware for some Intel® Processors may allow escalation of privilege and/or denial of service. Intel is releasing firmware updates to mitigate these potential vulnerabilities.
- Vulnerability Details:

  CVEID: **CVE-2020-0528**
  Improper buffer restrictions in BIOS firmware for 7th, 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access.

  CVEID: **CVE-2020-0529**
  Description: Improper initialization in BIOS firmware for 8th, 9th and 10th Generation Intel(R) Core(TM) Processor families may allow an unauthenticated user to potentially enable escalation of privilege via local access.
- Affected Products:
  - 7th / 8th / 9th / 10th Generation Intel® Core™ processors
- **Intel® security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00322.html

STATUS

- **IN PROCESS**

RESOLUTION

Dynabook Inc. continues to work with Intel® on updates with new versions available per guidance from Intel's Security Issue Update.

As soon as the related **BIOS packages** published by Dynabook Inc. containing updated Intel Firmware (Microcode update) to mitigate this potential vulnerability is available, visit http://emea.dynabook.com/support/drivers/laptops/ for download.

Special Register Buffer Data Sampling Advisory (Intel-SA-00320)

INTRODUCTION

Special Register Buffer Data Sampling Advisory

VULNERABILTY SUMMARY

INTEL-SA-00320

- A potential security vulnerability in some Intel® Processors may allow information disclosure. Intel® is releasing firmware updates to mitigate this potential vulnerability.
- Vulnerability Details:
  CVEID: **CVE-2020-0543**

  Description: Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
- **Intel® security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00320.html

STATUS

- **IN PROCESS**

RESOLUTION

Dynabook Inc. continues to work with Intel® on updates with new versions available per guidance from Intel's Security Issue Update.

As soon as the related **BIOS packages** published by Dynabook Inc. containing updated Intel® Firmware (Microcode update) to mitigate this potential vulnerability is available, visit http://emea.dynabook.com/support/drivers/laptops/ for download.

2020.1 IPU – Intel® CSME, SPS, TXE, AMT, ISM and DAL Advisory (Intel-SA-00295)

INTRODUCTION

2020.1 IPU – Intel® CSME, SPS, TXE, AMT, ISM and DAL Advisory

VULNERABILTY SUMMARY

INTEL-SA-00295

- Potential security vulnerabilities in Intel® Converged Security and Manageability Engine (CSME), Intel® Server Platform Services (SPS), Intel® Trusted Execution Engine (TXE), Intel® Active Management Technology (AMT), Intel® Standard Manageability (ISM) and Intel® Dynamic Application Loader (DAL) may allow escalation of privilege, denial of service or information disclosure. Intel® is releasing firmware and software updates to mitigate these potential vulnerabilities.

- Vulnerability Details:

  CVEID: For a complete list of CVE ID's and related descriptions, please refer to https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html

- Affected Products:

  Intel® CSME Versions 11.0 through 11.8.76, 11.10 through 11.12.76, 11.20 through 11.22.76, 12.0 through 12.0.63, 13.0 through 13.0.31, 14.0 through 14.0.32, 14.5.11.
  Intel® CSME and Intel® AMT before versions 11.8.77, 11.12.77, 11.22.77, 12.0.64, 13.0.32, 14.0.33, 14.5.12.

- **Intel® security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html

STATUS

- **IN PROCESS**

RESOLUTION

Intel® Skylake, Kabylake, Kabylake-R platforms	→	Intel® ME FW package available (link to our download page below)
Intel® Comet Lake platforms	→	Intel® ME FW package available (distribution through Microsoft Windows Update)
Intel® Whiskey Lake platforms	→	ETA unknown (issue found during evaluation). Dynabook Inc. co-work with Intel® to fix the issue.

Please visit http://emea.dynabook.com/support/drivers/laptops/ to download the related package published by Dynabook Inc. After downloading the package, click execute and follow instructions on screen.

Intel® PROSet/Wireless WiFi Software Advisory (Intel-SA-00338)

INTRODUCTION

Intel® PROSet/Wireless WiFi Software Advisory

VULNERABILTY SUMMARY

INTEL-SA-00338

- Potential security vulnerabilities in some Intel® PROSet/Wireless WiFi products may allow escalation of privilege or denial of service. Intel is releasing software updates to mitigate these potential vulnerabilities.
- Vulnerability Details:

  CVEID: **CVE-2020-0557**
  Insecure inherited permissions in Intel(R) PROSet/Wireless WiFi products on Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.
  CVEID: **CVE-2020-0558**
  Improper buffer restrictions in kernel mode driver for Intel(R) PROSet/Wireless WiFi products on Windows 10 may allow an unprivileged user to potentially enable denial of service via adjacent access.

- Affected Products: Intel® PROSet/Wireless WiFi software for the following products before version 21.70
  Intel® Wi-Fi AX201 / AX200 / AC 9560 / AC 9462 / AC 9461 / AC 9260 / AC 8265 / AC 8260 / AC 3168 / 7265 (Rev D) Family / AC 3165
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00338.html

STATUS

- **RESOLVED**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

Latest available software can be obtained from Intel (https://www.intel.com/content/www/us/en/support/articles/000005634/network-and-i-o/wireless-networking.html).

To download the latest software published by Dynabook Inc., please visit http://emea.dynabook.com/support/drivers/laptops/ for download or check **Microsoft® Windows Update function** to obtain related packages.

Intel® Snoop Assisted L1D Sampling Advisory (Intel-SA-00330)

INTRODUCTION

Intel® Snoop Assisted L1D Sampling Advisory

VULNERABILTY SUMMARY

INTEL-SA-00330

- A potential security vulnerability in some Intel® Processors may allow information disclosure.
- Vulnerability Details:

  CVEID: **CVE-2020-0550**
  Improper data forwarding in some data cache for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00330.html

STATUS

- **PLEASE CHECK INFORMATION IN RESOLUTION SECTION**

RESOLUTION

This potential vulnerability is mitigated by using Virtual Machine Manager with the L1TF mitigations applied. For more information see L1TF. Intel is not recommending any new or additional mitigations for Operating Systems.

Additional technical details about this vulnerability can be found at:

https://software.intel.com/security-software-guidance/insights/deep-dive-snoop-assisted-l1-data-sampling

Intel® Processor Graphics Advisory (Intel-SA-00315)

INTRODUCTION

Intel® Processor Graphics Advisory

VULNERABILTY SUMMARY

INTEL-SA-00315

- Potential security vulnerabilities in Intel® Graphics Drivers may allow escalation of privilege, denial of service and/or information disclosure. Intel is releasing software updates to mitigate these potential vulnerabilities.
- Vulnerability Details:
  - CVEID: CVE-2020-0504
  - CVEID: CVE-2020-0516
  - CVEID: CVE-2020-0519
  - CVEID: CVE-2020-0520
  - CVEID: CVE-2020-0505
  - CVEID: CVE-2020-0501
  - CVEID: CVE-2020-0565
  - CVEID: CVE-2020-0514
  - CVEID: CVE-2020-0515
  - CVEID: CVE-2020-0508
  - CVEID: CVE-2020-0511
  - CVEID: CVE-2020-0503
  - CVEID: CVE-2020-0567
  - CVEID: CVE-2020-0502
  - CVEID: CVE-2020-0507
  - CVEID: CVE-2020-0517
  - CVEID: CVE-2020-0506
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00315.html

STATUS

- **RESOLVED**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

As soon as the related **Intel® Processor Graphics Driver** published by Dynabook Inc. is available, please visit http://emea.dynabook.com/support/drivers/laptops/ for download or check **Microsoft® Windows Update function** to obtain related packages.

Intel® Optane™ DC Persistent Memory Module Management Software Advisory (Intel-SA-00326)

INTRODUCTION

Intel® Optane™ DC Persistent Memory Module Management Software Advisory

VULNERABILTY SUMMARY

INTEL-SA-00326

- A potential security vulnerability in Intel® Optane™ DC Persistent Memory Module Management Software may allow escalation of privilege and denial of service. Intel is releasing software updates to mitigate this potential vulnerability.
- Vulnerability Details:

  CVEID: **CVE-2020-0546**

  Description: Unquoted service path in Intel(R) Optane(TM) DC Persistent Memory Module Management Software before version 1.0.0.3461 may allow an authenticated user to potentially enable escalation of privilege and denial of service via local access.
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00326.html

STATUS

- **RESOLVED**

RESOLUTION

Intel recommends updating Intel® Optane™ DC Persistent Memory Module Management Software to 1.0.0.3461 or later.

Updates are available for download at this location: https://downloadcenter.intel.com/download/29380/DCPM-Software-for-Intel-Optane-DC-Persistent-Memory-for-Windows-Server-2019

Intel® Processors Load Value Injection Advisory (Intel-SA-00334)

INTRODUCTION

Intel® Processors Load Value Injection Advisory

VULNERABILTY SUMMARY

INTEL-SA-00334

- Potential security vulnerabilities in some Intel® Processors may allow information disclosure. Intel and others are releasing software updates to mitigate these potential vulnerabilities.
- Vulnerability Details:

  CVEID: **CVE-2020-0551**
  Description: Load value injection in some Intel(R) Processors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00334.html

STATUS

- **PLEASE CHECK INFORMATION IN RESOLUTION SECTION**

RESOLUTION

Intel is not currently aware of any load value injection-specific universal or non universal gadget for Operating System from Application, VMM from VM, between guests in Virtualized environments, between different application and inside an application and is not releasing additional mitigations for these environments. As a best practice, Intel recommends that users update to the latest Operating System and VMM provided by your system vendors. For application developers or system administrators that wish to consider additional mitigations tailored to their specific threat models, additional information is available here, which contains additional technical details about this issue and mitigations.
For further details, please check above Intel security advisory note.

Intel® Processor Data Leakage Advisory (Intel-SA-00329)

INTRODUCTION

Intel® Processor Data Leakage Advisory

VULNERABILTY SUMMARY

INTEL-SA-00329

- Potential security vulnerabilities in some Intel® Processors may allow information disclosure. Intel is releasing firmware updates to mitigate these potential vulnerabilities.
- CVE-2020-0548
  - Description: *Cleanup errors in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.*
- CVE-2020-0549
  - Description: *Cleanup errors in some data cache evictions for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.*
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00329.html

STATUS

- OPEN

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

As soon as the related **BIOS packages** published by Dynabook Inc. containing updated Intel Firmware (Microcode update) to mitigate this potential vulnerability is available, visit http://emea.dynabook.com/support/drivers/laptops/ for download.

Intel® Processor Graphics Advisory (Intel-SA-00314)

INTRODUCTION

Intel® Processor Graphics Advisory

VULNERABILITY SUMMARY

INTEL-SA-00314

- A potential security vulnerability in Intel® Processor Graphics may allow information disclosure. Insufficient control flow in certain data structures for some Intel(R) Processors with Intel(R) Processor Graphics may allow an unauthenticated user to potentially enable information disclosure via local access. Intel recommends updating Intel® Processor Graphics Driver for Windows* (Windows OS Driver version):
  - *Version: 26.20.100.7209 or higher / 15.45.x.5077 or higher / 15.40.x.5107 or higher / 15.36.x.5117 or higher / 15.33.x.5100 or higher*
  - *Platforms based on Ivy Bridge, Bay Trail and Haswell do not have full mitigations at this time for the Windows OS. Updating the drivers for these platforms per recommendation on Intel security center advisory will substantively reduce the potential attack surface. Intel is working on full mitigations for these platforms and dynabook will make them available once they are validated.*
- CVE-2019-14615
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00314.html

STATUS

- **OPEN**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

As soon as the related **Intel® Processor Graphics Driver** published by Dynabook Inc. is available, please visit http://emea.dynabook.com/support/drivers/laptops/ for download.

Intel® RST Advisory (Intel-SA-00324)

INTRODUCTION

Intel® RST Advisory

VULNERABILITY SUMMARY

INTEL-SA-00324

- A potential security vulnerability in the Intel® Rapid Storage Technology (RST) may allow escalation of privilege. Improper permissions in the executable for Intel(R) RST before version 17.7.0.1006 may allow an authenticated user to potentially enable escalation of privilege via local access.
- CVE-2019-14568
- Intel security center advisory: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00324.html

STATUS

- **RESOLVED**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

To **download the Intel RST driver v17.7.0.1006 or later** published by Dynabook Inc., visit http://emea.dynabook.com/support/drivers/laptops/

OVERVIEW | BIOS RELEASE SCHEDULE

Please see next slides for details about each Security Advisory

			Intel-SA-00220		Intel-SA-00260		Intel-SA-00270		Intel-SA-00317	
Comet Lake	Portégé | Tecra	A30-G | A40-G | X30L-G	Target Date	FCS*	Target Date	FCS*	Target Date	FCS*	Target Date	Available
			BIOS Version	-	BIOS Version	-	BIOS Version	-	BIOS Version	v2.00
Whiskey Lake	Portégé | Tecra	X30-F | X40-F | X50-F	Target Date	Available	Target Date	FCS*	Target Date	Available	Target Date	Available
			BIOS Version	v2.40	BIOS Version	-	BIOS Version	v2.40	BIOS Version	v2.70
Kabylake-R	Portégé	X30T-E | WT30-E	Target Date	Available	Target Date	Available	Target Date	N/A	Target Date	Available
			BIOS Version	v2.40	BIOS Version	v2.40	BIOS Version	N/A	BIOS Version	v2.50
	Satellite Pro | Tecra	A50-E | R50-E | Z50-E	Target Date	Available	Target Date	Available	Target Date	N/A	Target Date	Available
			BIOS Version	v2.60	BIOS Version	v2.60	BIOS Version	N/A	BIOS Version	v2.60
	Satellite Pro | Tecra	A50-EC | R50-EC	Target Date	Available	Target Date	Available	Target Date	N/A	Target Date	Available
			BIOS Version	v2.10	BIOS Version	v2.10	BIOS Version	N/A	BIOS Version	v2.10
	Portégé | Tecra	X30-E | X40-E	Target Date	Available	Target Date	Available	Target Date	N/A	Target Date	Available
			BIOS Version	v2.30	BIOS Version	v2.30	BIOS Version	N/A	BIOS Version	v2.30
	Portégé	Z30-E	Target Date	Available	Target Date	Available	Target Date	N/A	Target Date	Available
			BIOS Version	v1.80	BIOS Version	v1.80	BIOS Version	N/A	BIOS Version	v1.80
	Portégé | Tecra	R30-E | A40-E	Target Date	2020/2/E	Target Date	2020/2/E	Target Date	N/A	Target Date	2020/2/E
			BIOS Version	v1.40	BIOS Version	v1.40	BIOS Version	N/A	BIOS Version	v1.40
	Portégé	X20W-E	Target Date	Available	Target Date	Available	Target Date	N/A	Target Date	Available
			BIOS Version	v2.20	BIOS Version	v2.20	BIOS Version	N/A	BIOS Version	v2.20
Kabylake	Portégé	X20W-D	Target Date	Available	Target Date	Available	Target Date	N/A	Target Date	Available
			BIOS Version	v3.60	BIOS Version	v3.60	BIOS Version	N/A	BIOS Version	v3.60
	Portégé | Tecra	X30-D | X40-D	Target Date	2020/2/E	Target Date	2020/2/E	Target Date	N/A	Target Date	2020/2/E
			BIOS Version	v3.80	BIOS Version	v3.80	BIOS Version	N/A	BIOS Version	v3.80
	Satellite Pro | Portégé | Tecra	A30-D | A40-D | A50-D | R50-D | Z50-D	Target Date	Available	Target Date	Available	Target Date	N/A	Target Date	Available
			BIOS Version	v5.20	BIOS Version	v5.20	BIOS Version	N/A	BIOS Version	v5.20
Skylake	Portégé | Tecra	Z30-C | Z40-C	Target Date	2020/2/E	Target Date	2020/2/E	Target Date	N/A	Target Date	2020/2/E
			BIOS Version	v7.00	BIOS Version	v7.00	BIOS Version	N/A	BIOS Version	v7.00
	Portégé	Z20T-C	Target Date	2020/2/E	Target Date	2020/2/E	Target Date	N/A	Target Date	2020/2/E
			BIOS Version	v6.40	BIOS Version	v6.40	BIOS Version	N/A	BIOS Version	v6.40
	Satellite Pro | Portégé | Tecra	A30-C | A40-C | A50-C | R50-C | Z50-C	Target Date	2020/2/E	Target Date	2020/2/E	Target Date	N/A	Target Date	2020/2/E
			BIOS Version	v8.50	BIOS Version	v8.50	BIOS Version	N/A	BIOS Version	v8.50
	dynaEdge	DE-100	Target Date	2020/2/E	Target Date	2020/2/E	Target Date	N/A	Target Date	2020/2/E
			BIOS Version	v3.10	BIOS Version	v3.10	BIOS Version	N/A	BIOS Version	v3.10

* FCS = First Customer Shipment (BIOS include fix already)

Unexpected Page Fault in Virtualized Environment Advisory (Intel-SA-00317)

INTRODUCTION

Unexpected Page Fault in Virtualized Environment Advisory

VULNERABILITY SUMMARY

INTEL-SA-00317

- A potential security vulnerability in multiple Intel® processors may allow escalation of privilege, denial of service, and/or information disclosure. Intel is releasing firmware updates to mitigate this potential vulnerability.
- **CVE-2019-14607**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00317.html

STATUS

- **IN PROCESS / SCHEDULE AVAILABLE**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

Please check overview page for BIOS release information and schedule

To **download BIOS packages** published by Dynabook Inc. containing updated Intel Firmware (Microcode update) to mitigate this potential vulnerability, visit http://emea.dynabook.com/support/drivers/laptops/

Intel® CSME Advisory (Intel-SA-00307)

INTRODUCTION

Intel® CSME Advisory

VULNERABILITY SUMMARY

INTEL-SA-00307

- A potential security vulnerability in CSME subsystem may allow escalation of privilege, denial of service, and information disclosure. Intel is releasing firmware updates to mitigate this potential vulnerability. Intel recommends updating to Intel® CSME versions 12.0.49, 13.0.21, and 14.0.11 or later.
- **CVE-2019-14598**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00307.html

STATUS

- **IN PROCESS**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

As soon as the related **Intel CSME FW package** published by Dynabook Inc. is available, please visit http://emea.dynabook.com/support/drivers/laptops/ to download the related package. After downloading the package, click execute and follow instructions on screen.

Intel® Processors Voltage Settings Modification Advisory (Intel-SA-00289)

INTRODUCTION

Intel® Processors Voltage Settings Modification Advisory

VULNERABILITY SUMMARY

INTEL-SA-00289

- A potential security vulnerability in some Intel® Processors may allow escalation of privilege and/or information disclosure. Intel has released firmware updates to system manufacturers to mitigate this potential vulnerability. Description: Improper conditions check in voltage settings for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege and/or information disclosure via local access.
- **CVE-2019-11157**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00289.html

STATUS

- **IN PROCESS**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

To **download the BIOS versions** published by Dynabook Inc. containing the related Intel Firmware (Microcode update), visit http://emea.dynabook.com/support/drivers/laptops/

2019.2 IPU – TSX Asynchronous Abort Advisory (Intel-SA-00270)

INTRODUCTION

2019.2 IPU – TSX Asynchronous Abort Advisory

VULNERABILITY SUMMARY

INTEL-SA-00270

- A potential security vulnerability in TSX Asynchronous Abort (TAA) for some Intel® Processors may allow information disclosure. TSX Asynchronous Abort condition on some CPUs utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
- **CVE-2019-11135**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00270.html

STATUS

- **IN PROCESS / SCHEDULE AVAILABLE**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

Please check overview page for BIOS release information and schedule

To **download BIOS packages** published by Dynabook Inc. containing updated Intel Firmware (Microcode update) to mitigate this potential vulnerability, visit http://emea.dynabook.com/support/drivers/laptops/

2019.2 IPU – Intel® Processor Graphics Update Advisory (Intel-SA-00260)

INTRODUCTION

2019.2 IPU – Intel® Processor Graphics Update Advisory

VULNERABILITY SUMMARY

INTEL-SA-00260

- A potential security vulnerability in Intel® Processor Graphics may allow denial of service. Intel is releasing software and firmware updates to mitigate this potential vulnerability.
- **CVE-2019-0154**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00260.html

STATUS

- **IN PROCESS / SCHEDULE AVAILABLE**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

Please check overview page for BIOS release information and schedule

To **download BIOS packages** published by Dynabook Inc. containing updated Intel Firmware (Microcode update) to mitigate this potential vulnerability, visit http://emea.dynabook.com/support/drivers/laptops/

Intel® Ethernet I218 Adapter Driver for Windows Advisory (Intel-SA-00253)

INTRODUCTION

Intel® Ethernet I218 Adapter Driver for Windows

VULNERABILITY SUMMARY

INTEL-SA-00253

- A potential security vulnerability in Intel® Ethernet I218 Adapter driver for Windows* 10 may allow information disclosure. Insufficient memory protection for Intel(R) Ethernet I218 Adapter driver for Windows* 10 before version 24.1 may allow an authenticated user to potentially enable information disclosure via local access.
- **CVE-2019-11096**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00253.html

STATUS

- **IN PROCESS**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

To **download the Intel LAN driver package** published by Dynabook Inc., visit http://emea.dynabook.com/support/drivers/laptops/

Intel® CSME, Intel® SPS, Intel® TXE, Intel® AMT, Intel® PTT and Intel® DAL Advisory (Intel-SA-00241)

INTRODUCTION

Intel® CSME, Intel® SPS, Intel® TXE, Intel® AMT, Intel® PTT and Intel® DAL Advisory

VULNERABILITY SUMMARY

INTEL-SA-00241

- Potential security vulnerabilities in Intel® Converged Security and Manageability Engine (CSME), Intel® Server Platform Services (SPS), Intel® Trusted Execution Engine (TXE), Intel® Active Management Technology (AMT), Intel® Platform Trust Technology (PTT) and Intel® Dynamic Application Loader (DAL) may allow escalation of privilege, denial of service or information disclosure. Intel is releasing firmware and software updates to mitigate these potential vulnerabilities.
- **For overview of CVE's, please check below Intel advisory web page**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00241.html

STATUS

- **IN PROCESS**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

To **download the firmware package TCH0670700B (supporting Skylake / Kabylake / Kabylake-R platforms)** published by Dynabook Inc. containing the related Intel Firmware (Microcode update), visit http://emea.dynabook.com/support/drivers/laptops/

* Whiskey Lake based platform package available soon

Microarchitectural Data Sampling Advisory (Intel-SA-00233)

INTRODUCTION

Intel Firmware 2018.4 QSR Advisory

VULNERABILITY SUMMARY

INTEL-SA-00233

- A potential security vulnerability in CPUs may allow information disclosure. Intel is releasing Microcode Updates (MCU) updates to mitigate this potential vulnerability.
- **CVE-2018-12126 | CVE-2018-12127 | CVE-2018-12130 | CVE-2019-11091**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html

STATUS

- **IN PROCESS**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

To **download the BIOS versions** published by Dynabook Inc. containing the related Intel Firmware (Microcode update), visit http://emea.dynabook.com/support/drivers/laptops/

Intel® SGX and Intel® TXT Advisory (Intel-SA-00220)

INTRODUCTION

Intel® SGX and Intel® TXT Advisory

VULNERABILITY SUMMARY

INTEL-SA-00220

- Potential security vulnerabilities in Intel® Software Guard Extensions (SGX) and Intel® Trusted Execution Technology (TXT) may allow escalation of privilege. Intel is releasing firmware updates to mitigate these potential vulnerabilities.
- **CVE-2019-0123 | CVE-2019-0124**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00220.html

STATUS

- **IN PROCESS / SCHEDULE AVAILABLE**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

Please check overview page for BIOS release information and schedule

To **download BIOS packages** published by Dynabook Inc. containing updated Intel Firmware (Microcode update) to mitigate this potential vulnerability, visit http://emea.dynabook.com/support/drivers/laptops/

Intel® CSME, Intel® SPS, Intel® TXE, Intel® DAL, and Intel® AMT 2019.1 QSR Advisory (Intel-SA-00213)

INTRODUCTION

Intel® CSME, Intel® SPS, Intel® TXE, Intel® DAL, and Intel® AMT 2019.1 QSR Advisory

VULNERABILITY SUMMARY

INTEL-SA-00213

- Multiple potential security vulnerabilities in Intel® Converged Security & Management Engine (Intel® CSME), Intel® Server Platform Services (Intel® SPS), Intel® Trusted Execution Engine Interface (Intel® TXE), Intel® Dynamic Application Loader (Intel® DAL), and Intel® Active Management Technology (Intel® AMT) may allow escalation of privilege, information disclosure, and/or denial of service. Intel is releasing Intel® CSME, Intel® SPS, Intel® TXE, and Intel® AMT updates to mitigate these potential vulnerabilities.

- **CVE-2019-0089 | CVE-2019-0090 | CVE-2019-0086 | CVE-2019-0091 | CVE-2019-0092 | CVE-2019-0093 | CVE-2019-0094 | CVE-2019-0096 | CVE-2019-0097 | CVE-2019-0098 | CVE-2019-0099 | CVE-2019-0153 | CVE-2019-0170**

- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00213.html

STATUS

- **RESOLVED**

RESOLUTION

Intel recommends users to update firmware for Intel® CSME before versions 11.8.65 (Skylake, Kabylake, Kabylake-R) and 12.0.35 (Whiskey Lake).
Please download the latest mitigated firmware packages via http://emea.dynabook.com/support/drivers/laptops/
and upgrade to this version.

Intel® Firmware 2018.4 QSR Advisory (Intel-SA-00191)

INTRODUCTION

Intel Firmware 2018.4 QSR Advisory

VULNERABILITY SUMMARY

INTEL-SA-00191

- Multiple potential security vulnerabilities in Intel firmware may allow for escalation of privilege, information disclosure or denial of service. Intel is releasing firmware updates to mitigate these potential vulnerabilities.
- **CVE-2018-12201 | CVE-2018-12202 | CVE-2018-12203 | CVE-2018-12204 | CVE-2018-12205**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00191.html

STATUS

- **RESOLVED**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

To **download the BIOS versions** published by Dynabook Inc. containing the related Intel Firmware (Microcode update), visit http://emea.dynabook.com/support/drivers/laptops/

Intel® Graphics Driver for Windows* 2018.4 QSR Advisory (Intel-SA-00189)

INTRODUCTION

Intel® Graphics Driver for Windows* 2018.4 QSR Advisory

VULNERABILITY SUMMARY

INTEL-SA-00189

- Multiple potential security vulnerabilities in Intel® Graphics Driver for Windows* may allow escalation of privileges, denial of service or information disclosure. Intel is releasing Intel® Graphics Driver for Windows* updates to mitigate these potential vulnerabilities.

- **CVE-2018-12209 | CVE-2018-12210 | CVE-2018-12211 | CVE-2018-12212 | CVE-2018-12213 | CVE-2018-12214 CVE-2018-12215 | CVE-2018-12216 | CVE-2018-12217 | CVE-2018-12218 | CVE-2018-12219 | CVE-2018-12220 CVE-2018-12221 | CVE-2018-12222 | CVE-2018-12223 | CVE-2018-12224 | CVE-2018-18089 | CVE-2018-18090 CVE-2018-18091**

- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00189.html

STATUS

- **RESOLVED**

RESOLUTION

Intel recommends to update Intel® Graphics Driver for Windows.

Dynabook Inc. released a platform based driver list. Please see **next slide** for details.

DYNABOOK INC. RELEASE SCHEDULE

Dynabook Inc. release information for Intel® Graphics Driver release for Windows* 2018.4 QSR Advisory (**INTEL-SA-00189**)

PLATFORM *	WINDOWS VERSION	DRIVER VERSION FOR SECURITY UPDATE	RELEASE STATUS	T-PACKAGE	VERSION NOTE
▪ **Kaby Lake / Kaby Lake-R** (Net New / DCH - UWP)	› Win10 RS4, RS5	› 24.20.100.6346	➲ **Released**	TCH0533300A	› 24.20.100.6346(100.6346)
	› Win10 RS3	› 24.20.100.6287	➲ **Released**	TCH0546900A	› 24.20.100.6287(100.6287)
▪ **Kaby Lake / Kaby Lake-R** (Legacy)	› Win10 RS2, RS3, RS4	› 24.20.100.6286	➲ **Released**	TCH0525800A	› 24.20.100.6286(100.6286)
	› Win10 RS1	› 23.20.16.4849	➲ **Released**	TCH0431900A	› 23.20.16.4849(15.60.1.4849)
▪ **Skylake**	› Win10 RS2, RS3, RS4, RS5	› 24.20.100.6286	➲ **Released**	TCH0525800A	› 24.20.100.6286(100.6286)
	› Win10 RS1	› 23.20.16.4849	➲ **Released**	TCH0431900A	› 23.20.16.4849(15.60.1.4849)
	› Win7, 8.1	› 21.20.16.5068	≈ **2019 / TBD**		
▪ **Broadwell**	› Win10	› 20.19.15.5070	➲ **Released**	TCH0612200A	› 20.19.15.5070(v15.40.43.64.5070)
	› Win7, 8.1 64bit	› 20.19.15.5063	➲ **Released**	TCH0549800A	› 20.19.15.5063(15.40.42.64.5063)
	› Win7 32bit	› 20.19.15.5063	➲ **Released**	TCH0549900A	› 20.19.15.5063(15.40.42.5063)
▪ **Braswell**	› Win10	› 20.19.15.5070	≈ **2019 / TBD**		
▪ **Haswell**	› Win10	› 20.19.15.5070	➲ **Released**	TCH0612200A	› 20.19.15.5070(v15.40.43.64.5070)
	› Win7, 8.1	› 10.18.14.5067	≈ **2019 / TBD**		
▪ **Cherry Trail**	› Win10	› 20.19.15.5070	≈ **2019 / TBD**		
	› Win8.1	› 20.19.15.5063	➲ **Released**	TCH0468600B	› 20.19.15.5063(15.40.42.64.5063)
▪ **Bay Trail**	› Win7, 8.1, 10	› 10.18.10.5069	≈ **2019 / TBD**		
▪ **Skylake (DTPC)**	› Win7, 8.1, 10	› 21.20.16.5068	≈ **2019 / TBD**		
▪ **Haswell (DTPC)**	› Win10	› 20.19.15.5070	≈ **2019 / TBD**		
	› Win7, 8.1	› 10.18.14.5067	≈ **2019 / TBD**		

* How to Find the Code Name for Intel® Processors

DOWNLOAD DRIVERS

Visit http://emea.dynabook.com/support/drivers/laptops/ to view and **download latest drivers** for your system.

Intel® CSME, SPS, Trusted Execution Engine / Intel® Active Management Technology 2018.4 QSR Advisory (Intel-SA-00185)

INTRODUCTION

Intel® CSME, Server Platform Services, Trusted Execution Engine and Intel® Active Management Technology 2018.4 QSR Advisory

VULNERABILITY SUMMARY

INTEL-SA-00185

- Multiple potential security vulnerabilities in Intel® CSME, Server Platform Services, Trusted Execution Engine and Intel® Active Management Technology may allow users to potentially escalate privileges, disclose information or cause a denial of service. Intel is releasing Intel® CSME, Server Platform Services, Trusted Execution Engine and Intel® Active Management Technology updates to mitigate these potential vulnerabilities.

- **CVE-2018-12188 | CVE-2018-12189 | CVE-2018-12190 | CVE-2018-12191 | CVE-2018-12192 | CVE-2018-12199**
  CVE-2018-12198 | CVE-2018-12208 | CVE-2018-12200 | CVE-2018-12187 | CVE-2018-12196 | CVE-2018-12185

- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00185.html

STATUS

- **RESOLVED**

RESOLUTION

Intel recommends users to install updated firmware which mitigates this issue. Please download the latest mitigated firmware packages via http://emea.dynabook.com/support/drivers/laptops/ and upgrade to this version:

1. Intel ME FW Update Tool Version: **V1.1.6.2** (**TCH0577600C**)
2. Intel AMT Software: **TCH0549100A / TCH0548500A / TCH0519800D**

Intel® PROSet/Wireless WiFi Software Advisory (Intel-SA-00182)

INTRODUCTION

A potential security vulnerability in Intel® PROSet/Wireless WiFi Software may allow escalation of privilege. Intel is releasing software updates to mitigate this potential vulnerability.

VULNERABILITY SUMMARY

INTEL-SA-00182

- Improper directory permissions in the ZeroConfig service in Intel(R) PROSet/Wireless WiFi Software before version 20.90.0.7 may allow an authorized user to potentially enable escalation of privilege via local access.
- **CVE-2018-12177**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00182.html

STATUS

- **RESOLVED**

RESOLUTION

Please install Intel Wireless LAN driver 20.90 for Intel PROSet/Wireless vulnerability (**TCH0436100G**) or later.

To **download the Intel® PROSet / WiFi Software** published by Dynabook Inc., visit http://emea.dynabook.com/support/drivers/laptops/

Intel® Converged Security Management Engine (Intel® CSME) Q2'2018 Security Release (Intel-SA-00125, Intel-SA-00141 and Intel-SA-00142)

INTRODUCTION

Intel® Converged Security Management Engine (Intel® CSME) Q2'2018 Security Release.

VULNERABILITY SUMMARY

INTEL-SA-00125

- Security Advisory intended for **CVE-2018-3655**

INTEL-SA-00141

- Security Advisory intended for **CVE-2018-3657, CVE-2018-3658, CVE-2018-3616, CVE-2018-3657**

INTEL-SA-00142

- Security Advisory intended for **CVE-2018-3659**

STATUS

- **RESOLVED**

RESOLUTION

Intel recommends users to install updated firmware which mitigates this issue. Please download the latest mitigated firmware packages via http://emea.dynabook.com/support/drivers/laptops/ and upgrade to this version:

1. Intel AMT Software: **V11.8.55.3510** (**TCH0494500C**)
2. Intel ME FW Update Tool Version: **V1.1.5.1** or later (**TCH0513900B**)

Note: *Ensure to apply AMT Software **TCH0494500C** prior to Intel ME FW update **TCH0513900B***

Power Management Controller (PMC) Security Vulnerability in Systems using specific Intel® Converged Security and Management Engine (CSME) or Intel® Server Platform Services firmware versions (Intel-SA-00131)

INTRODUCTION

Security researchers have identified a speculative execution side-channel method called L1 Terminal Fault (L1TF).

VULNERABILITY SUMMARY

INTEL-SA-00131

Security Advisory intended for **CVE-2018-3643**

- A vulnerability in Power Management Controller firmware in systems using specific Intel® Converged Security and Management Engine (CSME) prior to versions 11.8.55, 11.11.55, 11.21.55, 12.0.5 or Intel® Server Platform Services firmware versions prior to 4.x.05 allows an attacker with administrative privileges to uncover certain platform secrets via local access.

STATUS

- **RESOLVED**

RESOLUTION

Intel recommends users to install updated firmware which mitigates this issue. Please download the latest mitigated firmware packages via http://emea.dynabook.com/support/drivers/laptops/ and upgrade to this version:

1. Intel AMT Software: **V11.8.55.3510** (**TCH0494500C**)
2. Intel ME FW Update Tool Version: **V1.1.5.1** or later (**TCH0513900B**)

Note: *Ensure to apply AMT Software **TCH0494500C** prior to Intel ME FW update **TCH0513900B***

INTRODUCTION

Power Management Controller (PMC) Security Vulnerability in Systems using specific Intel® Converged Security and Management Engine (CSME) or Intel® Server Platform Services firmware versions.

VULNERABILITY SUMMARY

INTEL-SA-00161

- Security researchers have identified a speculative execution side-channel method called L1 Terminal Fault (L1TF). This method impacts select microprocessor products supporting Intel® Software Guard Extensions (Intel® SGX). Further investigation by Intel has identified two related applications of L1TF with the potential to impact additional microprocessors, operating systems, system management mode, and virtualization software. If used for malicious purposes, this class of vulnerability has the potential to improperly infer data values from multiple types of computing devices.

- **CVE-2018- 3615 | CVE-2018- | CVE-2018- 3646**

- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html

STATUS

- **RESOLVED**

RESOLUTION

Intel has worked with operating system vendors, equipment manufacturers, and other ecosystem partners to develop platform firmware and software updates that can help protect systems from these methods. This includes the release of updated Intel microprocessor microcode to our customers and partners. This microcode was previously released as part of Intel-SA-00115.

Note: For **BIOS releases** containing related microcode update, please **check** Intel-SA-00115 **status**

Intel® AMT 9.x/10.x/11.x Security Review Cumulative Update and Intel® ME 11.x issue (Intel-SA-00112 & Intel-SA-00118)

INTRODUCTION

Intel Q1'18 Intel® Active Management Technology 9.x/10.x/11.x Security Review Cumulative Update (**Intel-SA-00112**) & Intel® Management Engine 11.x issue (**Intel-SA-00118**)

VULNERABILITY SUMMARY

INTEL-SA-00112

- The issues affect Intel® Active Management Technology 3.x/4.x/5.x/6.x/7.x/8.x/9.x/10.x/11.x used in corporate PCs (Intel® vPro, Intel® AMT), IOT devices, workstations and servers. These firmware versions may be found on certain products.
- **CVE-2018- 3628 | CVE-2018- 3629 | CVE-2018- 3632**
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00112.html

INTEL-SA-00112

- **CVE-2018-3627:** The issues affects Intel® ME 11.x used in consumer/corporate PCs (Intel® vPro or not, Intel® AMT or not), IOT devices and workstation. The affected firmware version may be found on certain products.
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00112.html

STATUS

- **RESOLVED**

RESOLUTION

Intel recommends users to install updated firmware which mitigates this issue.

Please download the **latest mitigated Intel Management Engine firmware version (Dynabook Inc. package TCH0486400A / V1.1.4.0 or later)** from http://emea.dynabook.com/support/drivers/laptops/ and upgrade to this version.

Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method (Intel-SA-00088 and Intel-SA-00115)

INTRODUCTION

Side channel methods techniques may allow an attacker to gain information through observing the system, such as measuring micro architectural properties.
Side channel methods: branch target injection, bounds check bypass, and speculative store bypass.

VULNERABILITY SUMMARY

INTEL-SA-00188 and Intel-SA-00115

- Security researchers disclosed several software analysis methods that, when used for malicious purposes, have the potential to improperly gather sensitive data from many types of computing devices with many different vendors processors and operating systems. Vulnerabilities have nicknamed as "**Spectre**" and "**Meltdown**".

- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00088.html
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html
- **Microsoft Security Update Guide:** https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

SPECTRE	CVE-2017-5753 – Bounds check bypass	Variant 1	Require OS update
	CVE-2017-5715 – Branch target injection	Variant 2	Require OS update and BIOS Update
	CVE-2019-1125 - Speculative Access Memory	Variant 1	Require OS update
MELTDOWN	CVE-2017-5754 – Rogue data cache load	Variant 3	Require OS update
	CVE-2018-3640 – Rogue System Register Read	Variant 3a	Require BIOS update
	CVE-2018-3639 – Speculative Store Bypass	Variant 4	Require BIOS update

STATUS

- **RESOLVED**

RESOLUTION

Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update. To obtain related **BIOS versions** from Dynabook Inc., visit http://emea.dynabook.comgeneric/recently-reported-vulnerabilities-microprocessors/

Unsafe Opcodes exposed in Intel SPI based products (Intel-SA-00087)

INTRODUCTION

Configuration of SPI Flash in platforms based on multiple Intel CPUs allows a local attacker to alter the behavior of the SPI Flash, potentially leading to a Denial of Service. This issue has been root-caused, and the mitigation has been validated and is available.

VULNERABILITY SUMMARY

INTEL-SA-000087

- Configuration of SPI Flash in platforms based on multiple, Intel platforms allows a local attacker to alter the behavior of the SPI Flash, potentially leading to a Denial of Service. Intel identified this issue internally. Issue is root-caused, and the mitigation is known and available. To Intel's knowledge, the issue has not been seen externally.
- **CVE-2017-5703** – Intel CPU SPI Flash Denial of Service
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00087.html

STATUS

- **RESOLVED**

RESOLUTION

Dynabook Inc. includes this fix in the similar BIOS versions, which is released for "**Spectre**" and "**Meltdown**" vulnerability.

To obtain the related **BIOS versions** published by Dynabook Inc., visit http://emea.dynabook.com/generic/recently-reported-vulnerabilities-microprocessors/ or download via http://emea.dynabook.com/support/drivers/laptops/

Intel(R) Graphics Driver vulnerabilities (Intel-SA-00089 and Intel-SA-00095)

INTRODUCTION

Pointer dereference in subsystem in Intel(R) Graphics Driver allows unprivileged user to elevate privileges via local access. Type Confusion in Content Protection HECI Service in Intel® Graphics Driver allows unprivileged user to elevate privileges via local access.

VULNERABILITY SUMMARY

INTEL-SA-00089

- The Intel® Graphics Drivers for Windows Code can fail to adequately validate a pointer input. This may lead to modification of kernel memory and a potential for an escalation of privilege. Reference **CVE-2017-5727**.
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00089.html

INTEL-SA-00095

- The Intel® Content Protection HECI Service has a Type Confusion vulnerability which potentially can lead to a privilege escalation. The HECI service software is distributed as part of the Intel Graphics Driver, and is used by the graphics driver to provide premium content playback services.
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00095.html

STATUS

- **RESOLVED**

RESOLUTION

- Intel highly recommends to **remove potentially vulnerable driver** versions and **upgrade to the latest mitigated driver** compatible with the system. Please **download the latest mitigated driver version** from http://emea.dynabook.com/support/drivers/laptops/ and upgrade to this version.

NOTE: If appropriate, we recommend to apply Intel® Graphics Drivers announced for Windows* 2018.4 QSR Advisory (**Intel-SA-00189**)

Potential vulnerability in Infineon TPM (Trusted Platform Module) used in Dynabook Inc. notebook products

INTRODUCTION

TPM is used for data encryption, creating a Public Key which is used alongside a Private Key. If the Public Key is accessed, there is a risk that the Private Key could potentially be identified.

VULNERABILITY SUMMARY

- If a Public Key generated by TPM and its paired Private Key are identified, a third party could impersonate a legitimate user and therefore decrypt data encrypted with a paired Public key and Private Key.
- Dynabook Inc. systems running **Infineon TPM v1.20 and v2.0** are **potentially affected**.

Additional information available from Infineon: https://www.infineon.com/cms/en/product/promopages/tpm-update/?redirId=59160
Additional information available from Microsoft: https://go.microsoft.com/fwlink/?linkid=852572

STATUS

- **RESOLVED**

RESOLUTION

Dynabook Inc. recommend to **immediately update the TPM firmware** if your system is potentially affected.

For details please access http://emea.dynabook.com/generic/potential-vulnerability-in-Infineon-TPM/

Intel AMT® Upgradable to Vulnerable Firmware, Intel Security Vulnerabilities Regarding Intel® Management Engine (ME), Intel® Server Platform Services (SPS), and Intel® Trusted Execution Engine (TXE) (Intel-SA-00082 and Intel-SA-00086)

INTRODUCTION

Intel AMT® Upgradable to Vulnerable Firmware (**Intel-SA-00082**)
Intel Q3'17 ME 6.x/7.x/8.x/9.x/10.x/11.x, SPS 4.0, and TXE 3.0 Security Review Cumulative Update (**Intel-SA-00086**)

VULNERABILITY SUMMARY

Intel-SA-00082

- Intel® Active Management Technology, Intel® Standard Manageability, and Intel® Small Business Technology firmware versions 11.0.25.3001 and 11.0.26.3000 anti-rollback will not prevent upgrading to firmware version 11.6.x.1xxx which is vulnerable to CVE-2017-5689 and can be performed by a local user with administrative privileges.
- **Intel security center advisory:** : https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00082.html

Intel-SA-00086

- In response to issues identified by external researchers, Intel has performed an in-depth comprehensive security review of its Intel® Management Engine (ME), Intel® Trusted Execution Engine (TXE), and Intel® Server Platform Services (SPS) with the objective of enhancing firmware resilience.
  As a result, Intel has identified several security vulnerabilities that could potentially place impacted platforms at risk. Systems using ME Firmware versions 6.x/7.x/8.x/9.x/10.x//11.0/11.5/11.6/11.7/11.10/11.20, SPS Firmware version 4.0, and TXE version 3.0 are impacted.

  Intel security center advisory: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00086.html

STATUS

- **RESOLVED**

RESOLUTION

Intel recommends users to install updated firmware which mitigates this issue.

The **updated firmware** can be obtained from https://support.dynabook.com/support/viewContentDetail?contentId=4015909

One or more Intel Products affected by the Wi-Fi Protected Access II (WPA2) protocol vulnerability (Intel-SA-00101)

INTRODUCTION

Researchers Mathy Vanhoef and Frank Piessens, from the University of Leuven, identified a series of vulnerabilities that affect the Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) standards.

VULNERABILITY SUMMARY

Intel-SA-00101

- These vulnerabilities are protocol-level vulnerabilities that affect a number of industry implementations of the standard in wireless infrastructure devices and wireless clients: https://papers.mathyvanhoef.com/ccs2017.pdf
  An attacker within range of an affected wireless access point (AP) and client may leverage these vulnerabilities to conduct attacks using susceptible data confidentiality protocols.

- CVEs relevant to Intel® Products and Technologies are:
  CVE-2017-13077, CVE-2017-13078, CVE-2017-13080, CVE-2017-13081

- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00101.html

STATUS

- **RESOLVED**

RESOLUTION

Intel highly recommends that customers **adopt the updates that include the mitigations** for the relevant CVE IDs referenced above.

Please download the latest mitigated driver version from http://emea.dynabook.com/support/drivers/laptops/ and upgrade to this version.

Intel Active Management Technology, Intel Small Business Technology, and Intel Standard Manageability Escalation of Privilege (Intel-SA-00075)

INTRODUCTION

Vulnerability in Intel® AMT, Intel® ISM, and Intel® Small Business Technology 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.

VULNERABILITY SUMMARY

Intel-SA-00075

- There are two ways this vulnerability may be accessed:
  - 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).
- The issue has been observed in Intel manageability firmware versions 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5, and 11.6 for Intel® Active Management Technology, Intel® Small Business Technology, and Intel® Standard Manageability. Versions before 6 or after 11.6 are not impacted. Intel highly recommends to update firmware. Firmware versions that resolve the issue have a four digit build number that starts with a “3” (X.X.XX.3XXX) Ex: 8.1.71.3608.
- **Intel security center advisory:** https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00075.html

STATUS

- **RESOLVED**

RESOLUTION

Firmware update for Dynabook Inc. products is available on http://emea.dynabook.comgeneric/Intel_AMT_vulnerability/

INTRODUCTION

The issue allows a local intruder to backdoor a system in a matter of seconds, even if the BIOS password, TPM Pin, Bitlocker and login credentials are in place.

VULNERABILITY SUMMARY

By selecting **Intel's Management Engine BIOS Extension (MEBx)**, intruders can log in using the default password "admin" if it has not been changed by the user.

STATUS

- **RESOLVED**

RESOLUTION

- **Changing default "admin" password** for Intel AMT will resolve the issue.

  For more information please refer to Security Best Practices of Intel® Active Management Technology Q&A

DOCUMENT REVISION INFO

- 16/09/2020
  - Vulnerability information for Intel-SA-00355 and Intel-SA-00337 added
  - Information for Intel-SA-00322 updated
- 05/08/2020
  - Vulnerability information for Intel-SA-00366 added
  - Information for Intel-SA-00295 updated
- 21/07/2020
  - Vulnerability information for Intel-SA-00322, Intel-SA-00320 and Intel-SA-00295 added
- 15/04/2020
  - Vulnerability information for Intel-SA-00338 added
- 30/03/2020
  - Vulnerability information for Intel-SA-00330 added
- 26/03/2020
  - Vulnerability information for Intel-SA-00315, Intel-SA-00326 and Intel-SA-00334 added
- 02/03/2020
  - Vulnerability information for Intel-SA-00324 and Intel-SA-00329 added
- 27/02/2020
  - Vulnerability information for Intel-SA-00307 added
  - BIOS Release Schedule related to Intel-SA-00220 | Intel-SA-00260 | Intel-SA-00270 | Intel-SA-00317 updated
- 18/12/2019
  - Vulnerability information for Intel-SA-00220, Intel-SA-00241 , Intel-SA-00253, Intel-SA-00260, Intel-SA-00270, Intel-SA-00289, Intel-SA-00317 and Intel-SA-00324 added
- 19/08/2019
  - Schedule for Intel-SA-00213 FW delayed
- 24/05/2019
  - Vulnerability information for Intel-SA-00213, Intel-SA-00223 added
  - Information for Intel-SA-00189 updated
- 21/03/2019
  - Vulnerability information for Intel-SA-00182, Intel-SA-00185, Intel-SA-00189 and Intel-SA-00191 added
- 18/09/2018
  - Vulnerability information for Intel-SA-00125, Intel-SA-00141 and Intel-SA-00142 added
  - Information for Intel-SA-00131 added
- 17/08/2018
  - Vulnerability information for Intel-SA-00161 added
- 09/07/2018
  - Vulnerability information for Intel-SA-00112 and Intel-SA-00118 added
  - Information for Intel-SA-00087, Intel-SA-00088 and Intel-SA-000115 updated
- 28/06/2018
  - Vulnerability information for Intel-SA-00087, Intel-SA-00088 and Intel-SA-00115 updated
- 25/04/2018
  - Vulnerability information for Intel-SA-00087 added
- 16/04/2018
  - Vulnerability information for Intel-SA-00089 and Intel-SA-00095 added
- 21/03/2018
  - Vulnerability information for Infineon TPM vulnerability added