SECURITY INFORMATION SUMMARY

The latest security information on 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
- FOR PREVIOUS TOPICS, PLEASE SEE ADDITIONAL DOCUMENT COVERING PERIOD 2017-2020

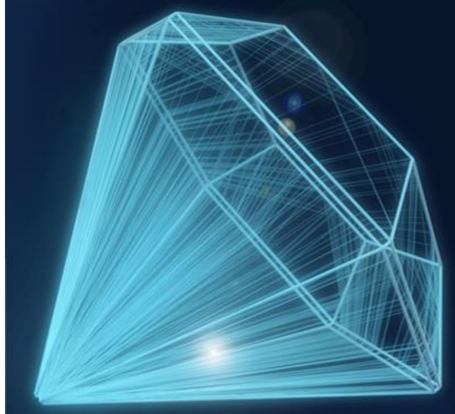
Last modified: December 01, 2021

© 2021 Dynabook Europe GmbH

SECURITY INFORMATION SUMMARY | CONTENTS

Overview of security vulnerabilities affecting Dynabook PC products

RELEASE DATE	VENDOR ID	VULNERABILTY DESCRIPTION	COMMENT
10. Nov 20	INTEL-SA-00381	2020.2 IPU - Intel® Processor Advisory	
10. Nov 20	INTEL-SA-00389	2020.2 IPU - Intel® RAPL Interface Advisory	
10. Nov 20	INTEL-SA-00391	2020.2 IPU – Intel® CSME, SPS, TXE, and AMT Advisory	
09. Nov 21	INTEL-SA-00393	Intel® Thunderbolt™ non-DCH Driver for Windows Advisory	
08. Jun 21	INTEL-SA-00401	Intel® Thunderbolt™ Controller Advisory	
08. Sep 20	INTEL-SA-00404	Intel® AMT and Intel® ISM Advisory	
09. Feb 21	INTEL-SA-00438	Intel® Graphics Drivers Advisory	
08. Jun 21	INTEL-SA-00442	2021.1 IPU - Intel® VT-d Advisory	
09. Feb 21	INTEL-SA-00448	Intel® PROSet/Wireless WiFi and Killer™ Driver Advisory	
09. Feb 21	INTEL-SA-00455	Intel® SGX Platform Advisory	
08. Jun 21	INTEL-SA-00459	2021.1 IPU – Intel® CSME, SPS and LMS Advisory	
08. Jun 21	INTEL-SA-00463	2021.1 IPU – BIOS Advisory	
08. Jun 21	INTEL-SA-00464	Intel® Processor Advisory	
08. Jun 21	INTEL-SA-00465	2021.1 IPU - Intel Atom® Processor Advisory	
08. Jun 21	INTEL-SA-00472	Intel® ProSet/Wireless WiFi Driver Advisory	
11. Mai 21	INTEL-SA-00473	Intel® PROSet/Wireless WiFi , Intel vPro® CSME WiFi and Killer™ WiFi Advisory Advisory	
10. Aug 21	INTEL-SA-00508	Intel® Graphics Drivers Advisory	
09. Nov 21	INTEL-SA-00509	Intel® PROSet/Wireless WiFi and Killer™ WiFi Software Advisory	
08. Jun 21	INTEL-SA-00520	Intel® Wireless Bluetooth® and Killer™ Bluetooth® Advisory	
09. Nov 21	INTEL-SA-00528	Intel® Processor Advisory	
09. Nov 21	INTEL-SA-00533	Intel® Thunderbolt™ DCH Driver for Windows Advisory	
09. Nov 21	INTEL-SA-00540	Intel® Wireless Bluetooth® and Killer™ Bluetooth® Advisory	
08. Jun 21	INTEL-SA-00545	Intel® Rapid Storage Technology Advisory	
12. Okt 21	INTEL-SA-00548	Intel® SGX SDK Advisory	Under investigation
09. Nov 21	INTEL-SA-00562	BIOS Reference Code Advisory	
09. Nov 21	INTEL-SA-00566	Intel® Graphics Drivers Advisory	



VULNERABILTY SUMMARY

- Potential security vulnerabilities in some Intel® Graphics Drivers may allow escalation of privilege or denial of service. Intel is releasing software updates to mitigate these potential vulnerabilities.

- **Vulnerability Details:**

  CVEID: **CVE-2021-0121**
  Description: Improper access control in the installer for some Intel(R) Iris(R) Xe MAX Dedicated Graphics Drivers for Windows 10 before version 27.20.100.9466 may allow authenticated user to potentially enable escalation of privilege via local access.

  CVEID: **CVE-2021-0120**
  Description: Improper initialization in the installer for some Intel(R) Graphics DCH Drivers for Windows 10 before version 27.20.100.9316 may allow an authenticated user to potentially enable denial of service via local access.

- **Affected Products:**

  Intel® Iris® Xe MAX Dedicated Graphics Drivers for Windows 10 before version 27.20.100.9466.
  Intel® Graphics DCH Drivers for Windows 10 before version 27.20.100.9316.
  Intel® Graphics non DCH Drivers for Windows 10 before version 100.9416.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00566.html

STATUS

- **RESOLVED**

RESOLUTION

- Intel recommends updating the affected Intel® Graphics Drivers to the latest versions.

  Update is available for download at this location:
  https://www.intel.com/content/www/us/en/download/19344/

Intel® Graphics Drivers Advisory

[**Intel-SA-00566**]

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- Potential security vulnerabilities in the BIOS reference code for some Intel® Processors may allow escalation of privilege. Intel is releasing firmware updates to mitigate these potential vulnerabilities.

- **Vulnerability Details:**

  CVEID: **CVE-2021-0157**
  Description: Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.

  CVEID: **CVE-2021-0158**
  Description: Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.

- **Affected Products:**

  Intel® Xeon® Processor E / E3 v6 Family, Intel® Xeon® Processor W Family
  3rd Generation Intel® Xeon® Scalable Processors
  11th / 10th / 7th Generation Intel® Core™ Processors
  Intel® Core™ X-series Processors, Intel® Celeron® Processor N Series
  Intel® Pentium® Silver Processor Series

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html

STATUS

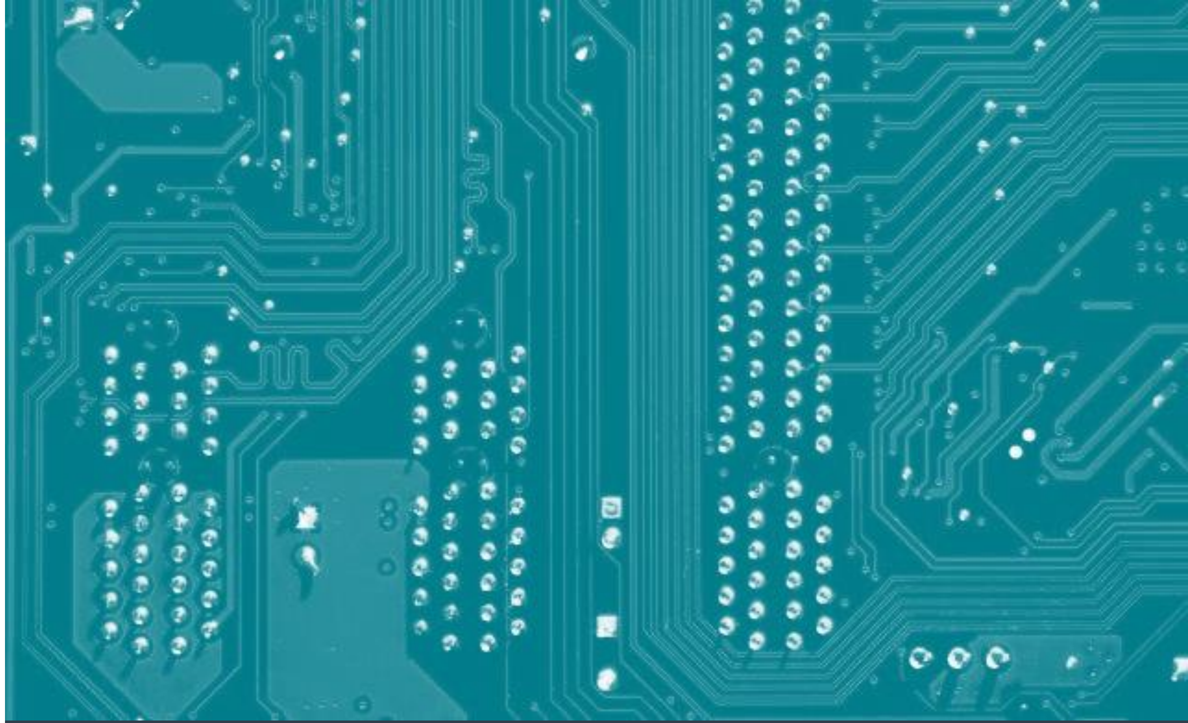
- **IN PROGRESS**

RESOLUTION

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

  Intel recommends that users of affected Intel® Processors update to the latest version provided by Dynabook Inc. that addresses these issues.

  Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available updates.



BIOS Reference Code Advisory

[Intel-SA-00562]

© 2021 Dynabook Europe GmbH

Intel® SGX SDK Advisory

[**Intel-SA-00548**]

VULNERABILTY SUMMARY

- A potential security vulnerability in Intel® Software Guard Extensions (SGX) Software Development Kit (SDK)applications compiled for SGX2-enabled processors may allow escalation of privilege. Intel is releasing software updates to mitigate this potential vulnerability.

- **Vulnerability Details:**

  CVEID: **CVE-2021-0186**

  Description: Improper input validation in the Intel(R) SGX SDK applications compiled for SGX2 enabled processors may allow a privileged user to potentially escalation of privilege via local access.

- **Affected Products:**

  Intel SGX SDK for Windows v2.12 and earlier / Intel SGX SDK for Linux v2.13 and earlier
  Intel® Processors supporting SGX2:

Code Name:	Ice Lake Xeon-SP (HCC, XCC)
Product Collection	3rd Gen Intel® Xeon® Scalable processor family
Code Name:	Ice Lake
Product Collection	10th Generation Intel® Core™ Processor Family
Code Name:	Gemini Lake
Product Collection	Intel® Pentium® Processor Silver Series, Intel® Celeron® Processor J / N Series

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html

STATUS

- **RESOLVED**

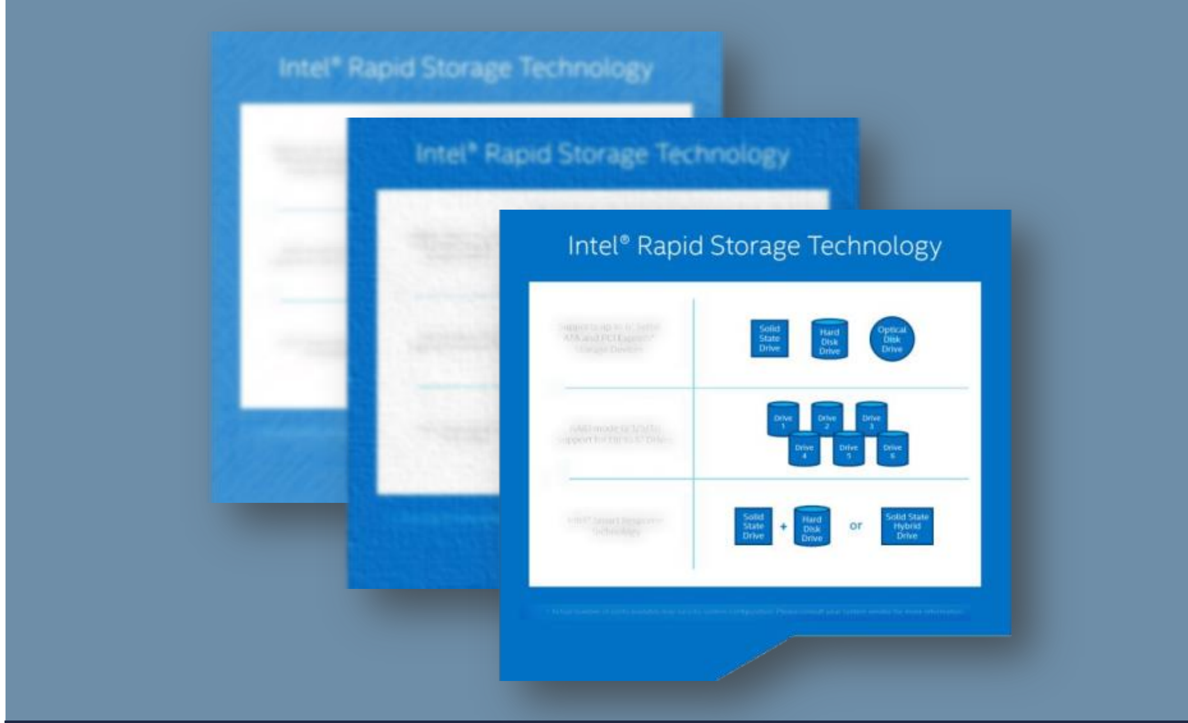
RESOLUTION

- Intel recommends updating the Intel® SGX SDK to the versions listed below. Enclaves built with the new Intel® SGX SDK version should increment the value of their ISVSVN field.

  Intel® SGX SDK for Windows to version 2.13 or later:
  https://registrationcenter.intel.com/en/products/download/3407/

  Intel® SGX SDK for Linux to version 2.14 or later:
  https://01.org/intel-software-guard-extensions/downloads

© 2021 Dynabook Europe GmbH



Intel® Rapid Storage Technology Advisory

[Intel-SA-00545]

VULNERABILTY SUMMARY

- A potential security vulnerability in the Intel® Rapid Storage Technology software may allow escalation of privilege. Intel is releasing software updates to mitigate this potential vulnerability.

- **Vulnerability Details:**

  CVEID: CVE-2021-0104

  Description: Uncontrolled search path element in the installer for the Intel(R) Rapid Storage Technology software, before versions 17.9.0.34, 18.0.0.640 and 18.1.0.24, may allow an authenticated user to potentially enable escalation of privilege via local access.

- **Affected Products:**

  - Intel® PROSet/Wireless WiFi products:
    Intel® Wi-Fi 6E AX210 / 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
  - Killer™ WiFi products:
    Killer™ Wi-Fi 6E AX1675 / Killer™ Wi-Fi 6 AX1650 / Killer™ Wireless-AC 1550

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00545.html

STATUS

- **RESOLVED**

RESOLUTION

- Windows OS:
  Intel recommends updating the affected Intel® Wireless Bluetooth® and Killer™ Bluetooth® products to version 22.60 or later.

  Windows 10 updates are available for download at this location:
  https://www.intel.com/content/www/us/en/support/articles/000005489/wireless/intel-wireless-products.html

  Updates for Killer™ drivers with Windows 10 are available for download at this location:
  https://www.intel.com/content/www/us/en/secure/design/confidential/products-and-solutions/wireless-and-modems/wireless-software/killer-performance-suite.html

© 2021 Dynabook Europe GmbH

Intel® Wireless Bluetooth® and Killer™ Bluetooth® Advisory

[Intel-SA-00540]

VULNERABILTY SUMMARY

- Potential security vulnerabilities in the installer for some Intel® Wireless Bluetooth® and Killer™ Bluetooth® products may allow escalation of privilege or denial of service. Intel is releasing software updates to mitigate these potential vulnerabilities..

- **Vulnerability Details:**

  CVEID: CVE-2021-0151
  Description: Improper access control in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable escalation of privilege via local access.

  CVEID: CVE-2021-0152
  Description: Improper verification of cryptographic signature in the installer for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products in Windows 10 may allow an authenticated user to potentially enable denial of service via local access.

- **Affected Products:**

  Intel® Rapid Storage Technology software before versions 17.9.1.1009.5, 18.0.3.1148.4 and 18.1.0.1028.2 with installer versions before 17.9.0.34, 18.0.0.640 and 18.1.0.24 respectively.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00540.html

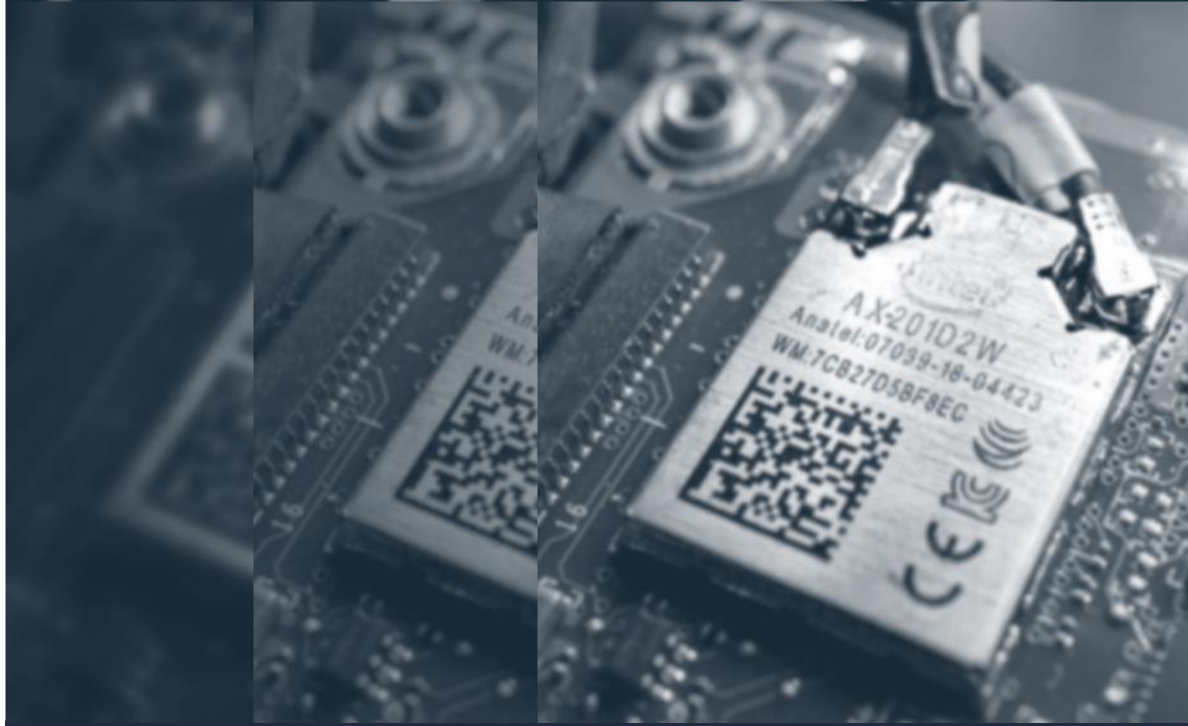
STATUS

- **RESOLVED**

RESOLUTION

- Intel recommends updating the Intel® Rapid Storage Technology software to versions 17.9.1.1009.5, 18.0.3.1148.4 and 18.1.0.1028.2 with installer versions before 17.9.0.34, 18.0.0.640 and 18.1.0.24 or higher.

  Updates are available for download at this location: Downloads for Intel® Rapid Storage Technology (Intel® RST)



© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- A potential security vulnerability in some Intel® Thunderbolt™ Declarative Componentized Hardware (DCH) Drivers for Windows may allow denial of service. Intel is releasing software updates to mitigate this potential vulnerability.

- **Vulnerability Details:**

  CVEID: **CVE-2021-0110**
  Description: Improper access control in some Intel(R) Thunderbolt(TM) Windows DCH Drivers before version 1.41.1054.0 may allow unauthenticated user to potentially enable denial of service via local access.

- **Affected Products:**

  Intel® Thunderbolt™ 3 and 4 Windows DCH Drivers before version 1.41.1054.0 for:
  - Intel® JHL6540 & JHL6340 & JHL6240
  - Intel® JHL7540 & JHL7440 & JHL7340
  - Intel® JHL8540 & JHL8440
  - Intel® 10th Gen & Intel® 11th Gen Core Processors with Thunderbolt™ Technology

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00533.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.

  Intel recommends updating Intel® Thunderbolt™ DCH Drivers for Windows to version 1.41.1094 or later. Updates are available for download at this location:

  https://www.intel.com/content/www/us/en/search.html?ws=recent#q=596793.

Intel® Thunderbolt™ DCH Driver for Windows Advisory

[Intel-SA-00533]

© 2021 Dynabook Europe GmbH

Intel® Processor Advisory

[Intel-SA-00528]

VULNERABILTY SUMMARY

- A potential security vulnerability in some Intel® Processors may allow escalation of privilege. Intel is releasing firmware updates to mitigate this potential vulnerability.

- **Vulnerability Details:**

  CVEID:

  - **CVE-2021-0146**

  Description:

  - Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.

- **Affected Products:**

  Intel® Pentium® Processor J Series, N Series, Intel® Celeron® Processor J Series, N Series,

  Intel® Atom® Processor A Series, Intel® Atom® Processor E3900 Series, Intel® Pentium® Processor N Series, Intel® Celeron® Processor N Series, Intel® Atom® Processor E3900 Series, Intel® Pentium® Processor Silver Series/ J&N Series, Intel® Pentium® Processor Silver Series/ J&N Series - Refresh, Intel® Atom® Processor C3000

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html

STATUS

- **IN PROGRESS**

RESOLUTION

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

  Intel recommends that users of affected Intel® Processors update to the latest version provided by Dynabook Inc. that addresses these issues.

  Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available updates.

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- Potential security vulnerabilities in Intel® Wireless Bluetooth® products and Killer™ Bluetooth® products may allow information disclosure. Intel is releasing firmware updates to mitigate these potential vulnerabilities.

- **Vulnerability Details:**

  CVEID: CVE-2020-26555 (Non-Intel issued)
  Intel Description (official wording not yet available): Improper access control in some Intel(R) Wireless Bluetooth(R) products in multiple operating systems and Killer(TM) Bluetooth(R) products in Windows 10 may allow an unauthenticated user to potentially enable information disclosure via adjacent access.

  CVEID: CVE-2020-26558 (Non-Intel issued)
  Intel Description (official wording not yet available): Improper authentication in some Intel(R) Wireless Bluetooth(R) products in multiple operating systems and Killer(TM) Bluetooth(R) products in Windows 10 may allow an unauthenticated user to potentially enable information disclosure via adjacent access.

- **Affected Products:**

  - Intel® Wireless Bluetooth® products:
    Intel® Wi-Fi AX210,AX201,AX200 / Intel® Wireless-AC9560,-AC9462,-AC9461,-AC9260 / Intel® Dual Band Wireless-AC 8265,-AC 8260,-AC 3168,-AC 3165 / Intel® Wireless 7265 (Rev D) Family
  - Killer™ Bluetooth® products:
    Killer™ Wi-Fi 6E AX1675 / Killer™ Wi-Fi 6 AX1650 / Killer™ Wireless-AC 1550

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00520.html

STATUS

- **RESOLVED**

RESOLUTION

- Intel recommends updating affected Intel® Wireless Bluetooth® and Killer™ Bluetooth® products to version 22.50 or later.

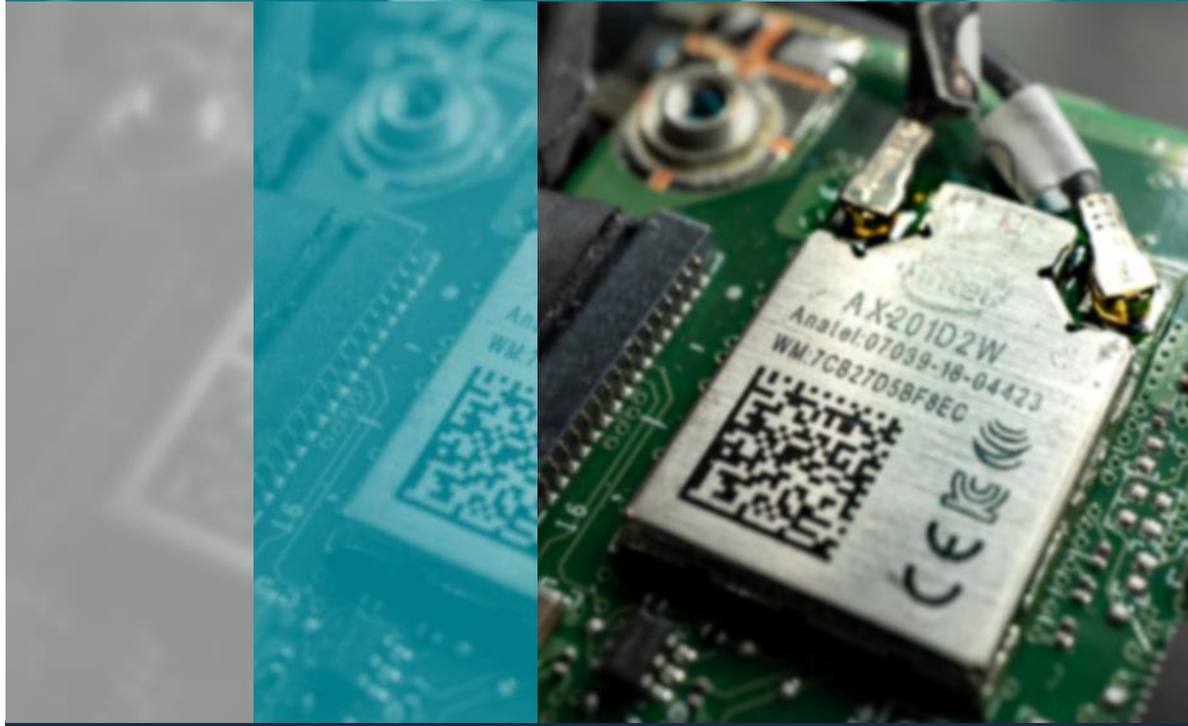
  For Windows* 10, updates are available for download at this location:
  https://www.intel.com/content/www/us/en/support.html

Intel® Wireless Bluetooth® and Killer™ Bluetooth® Advisory

[**Intel-SA-00520**]

© 2021 Dynabook Europe GmbH

dynabook



Intel® PROSet/Wireless WiFi and Killer™ WiFi Software Advisory

[Intel-SA-00509]

VULNERABILTY SUMMARY

- A potential security vulnerability in some Intel® ProSet/Wireless WiFi drivers may allow information disclosure and denial of service. Intel is releasing a software update to mitigate this potential vulnerability.

- **Vulnerability Details:**

  Please refer to the Intel security center advisory (link below) for details.

- **Affected Products:**

  - Intel® PROSet/Wireless WiFi products:
    Intel® Wi-Fi 6E AX210 / 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
  - Killer™ WiFi products:
    Killer™ Wi-Fi 6E AX1675 / Killer™ Wi-Fi 6 AX1650 / Killer™ Wireless-AC 1550

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00509.html

STATUS

- **RESOLVED**

RESOLUTION

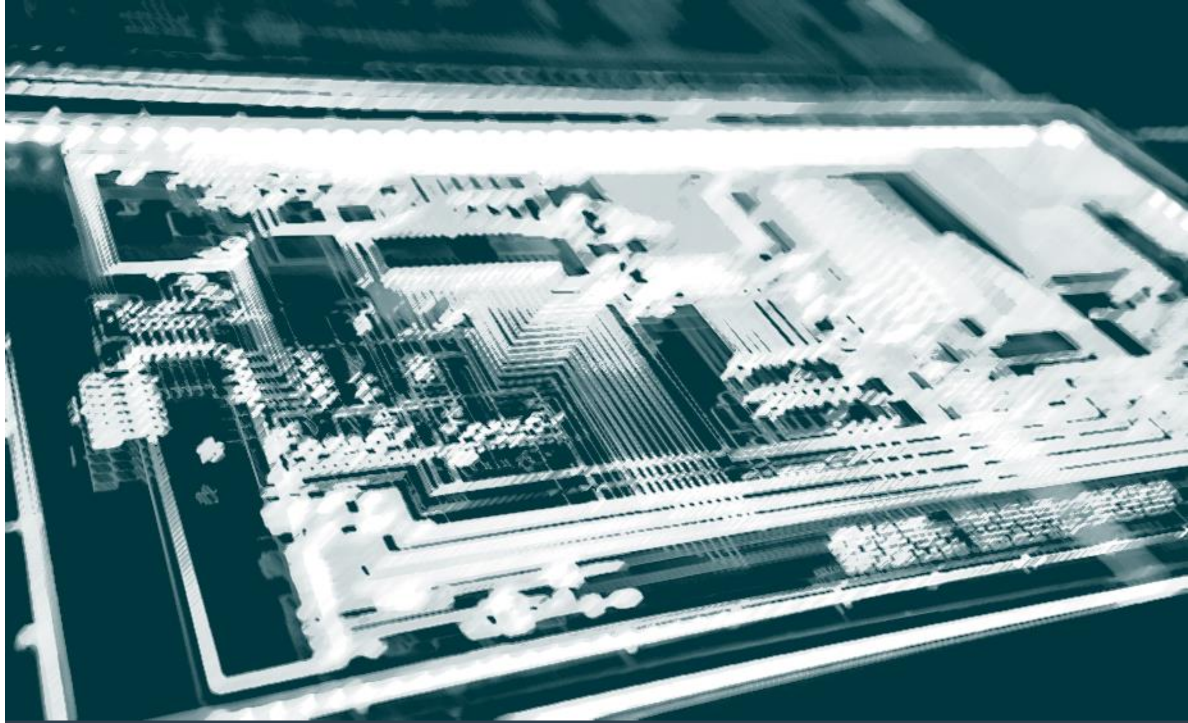
- Windows:
  Intel recommends updating Intel® PROSet/Wireless WiFi to version 22.40 or later.

  Updates are available for download at these locations:
  Intel® PROSet/Wireless WiFi driver:
  https://downloadcenter.intel.com/download/30434/Windows-10-Wi-Fi-Drivers-for-Intel-Wireless-Adapters

- Intel recommends updating Killer™ WiFi to version 2.4.1541 or later.

  Updates for Killer™ products are available for download at this location:
  https://downloadcenter.intel.com/download/30388/Intel-Killer-Performance-Suite

© 2021 Dynabook Europe GmbH



Intel® Graphics Drivers Advisory

[Intel-SA-00508]

VULNERABILTY SUMMARY

- Potential security vulnerabilities in some Intel® Graphics Drivers may allow escalation of privilege. Intel is releasing software updates to mitigate these potential vulnerabilities.

- **Vulnerability Details:**
  - **CVEID: CVE-2021-0061**
    Description: Improper initialization in some Intel(R) Graphics Driver before version 27.20.100.9030 may allow an authenticated user to potentially enable escalation of privilege via local access.
  - **CVEID: CVE-2021-0012**
    Description: Use after free in some Intel(R) Graphics Driver before version 27.20.100.8336, 15.45.33.5164, and 15.40.47.5166 may allow an authenticated user to potentially enable denial of service via local access.
  - **CVEID: CVE-2021-0062**
    Description: Improper input validation in some Intel(R) Graphics Drivers before version 27.20.100.8935 may allow an authenticated user to potentially enable escalation of privilege via local access.

- **Affected Products:**
  - Intel® Graphics Win10 Legacy Drivers before v**27.20.100.9171** / DCH Drivers before v**27.20.100.9030**
  - Intel® Graphics Driver for Windows before v**15.45.33.5164 /** before v**15.40.47.5166**

- **Intel® security center advisory:**
  - https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00508.html

STATUS

- **IN PROGRESS**

RESOLUTION

- Intel recommends that users of Intel® Graphics Windows 10 non-dch Driver update to the latest version provided by Dynabook Inc. that addresses these issues. Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available drivers.
- Intel recommends updating the Intel® Graphics Windows 10 DCH Drivers update to version 27.20.100.9030 or later. Updates are available for download at this location:
  https://downloadcenter.intel.com/download/30066/Intel-Graphics-Windows-10-DCH-Drivers
- Intel recommends updating the Intel® Graphics Driver for Windows update to version 15.45.33.5164 or later. Updates are available for download at this location:
  https://downloadcenter.intel.com/download/29972/Intel-Graphics-Driver-for-Windows-15-45-?product=80939
- Intel recommends updating the Intel® Graphics Driver for Windows update to version 15.40.47.5166 or later. Updates are available for download at this location:
  https://downloadcenter.intel.com/download/29971/Intel-Graphics-Driver-for-Windows-15-40-?product=80939

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- Potential security vulnerabilities in some Intel® PROSet/Wireless WiFi and Intel vPro® Converged Security and Management Engine (CSME) WiFi and Killer™ WiFi may allow denial of service. Intel is releasing firmware and software updates to mitigate these potential vulnerabilities.

- **Vulnerability Details:**

  CVEID: CVE-2020-24586 | CVE-2020-24587 | CVEID: CVE-2020-24588 (all Non-Intel issued)

- **Affected Products:**

  - Intel® PROSet/Wireless WiFi products:
    Intel® Wi-Fi AX210,AX201,AX200 / Intel® Wireless-AC9560,-AC9462,-AC9461,-AC9260 / Intel® Dual Band Wireless-AC 8265,-AC 8260,-AC 3168,-AC 3165 / Intel® Wireless 7265 (Rev D) Family
  - Intel vPRO® CSME WiFi products:
    Intel® Wi-Fi 6 AX201,AX200 / Intel® Dual Band-/Wireless-AC9560,-AC9260 / -AC8265,-AC8260
  - Killer™ WiFi products: Killer™ Wi-Fi 6E AX1675 / Killer™ Wi-Fi 6 AX1650 / Killer™ Wireless-AC 1550
  - Intel® PROSet/Wireless products: Intel® Wi-Fi 6 AX201 | AX200 | AC 9560 | AC 9462 | AC 9461
  - Killer™ products: Killer™ Wi-Fi 6 AX1650 | AC 1550

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00473.html

STATUS

- **RESOLVED**

RESOLUTION

- Intel recommends updating Intel® PROSet/Wireless WiFi to version 22.30 or later. Updates are available for download at this location: https://downloadcenter.intel.com/download/30208

  The 22.30.0 package installs the Windows 10 Wi-Fi drivers for the following Intel® Wireless Adapters:
  - 22.30.0.11 for AX210/AX201/AX200/9560/9260/9462/9461 (Only available in 64-bit version)
  - 20.70.21.2for 8265/8260 (Only available in 64-bit version)
  - 19.51.33.1 for 7265(Rev. D)/3165/3168

- Intel recommends that users of Intel® vPRO® CSME WiFi products update to the latest version provided by the system manufacturer that addresses these issues.

Intel® PROSet/Wireless WiFi and Killer™ Driver Advisory

[Intel-SA-00473]

© 2021 Dynabook Europe GmbH

dynabook

VULNERABILTY SUMMARY

- A potential security vulnerability in some Intel® ProSet/Wireless WiFi drivers may allow information disclosure and denial of service. Intel is releasing a software update to mitigate this potential vulnerability.

- **Vulnerability Details:**

  CVEID: CVE-2021-0105

  Description: Insecure inherited permissions in some Intel(R) ProSet/Wireless WiFi drivers may allow an authenticated user to potentially enable information disclosure and denial of service via adjacent access.

- **Affected Products:**

  - Intel® Wi-Fi 6 AX201
  - Intel® Wi-Fi 6 AX200
  - Intel® Wireless-AC 9560
  - Intel® Wireless-AC 9462
  - Intel® Wireless-AC 9461

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00472.html

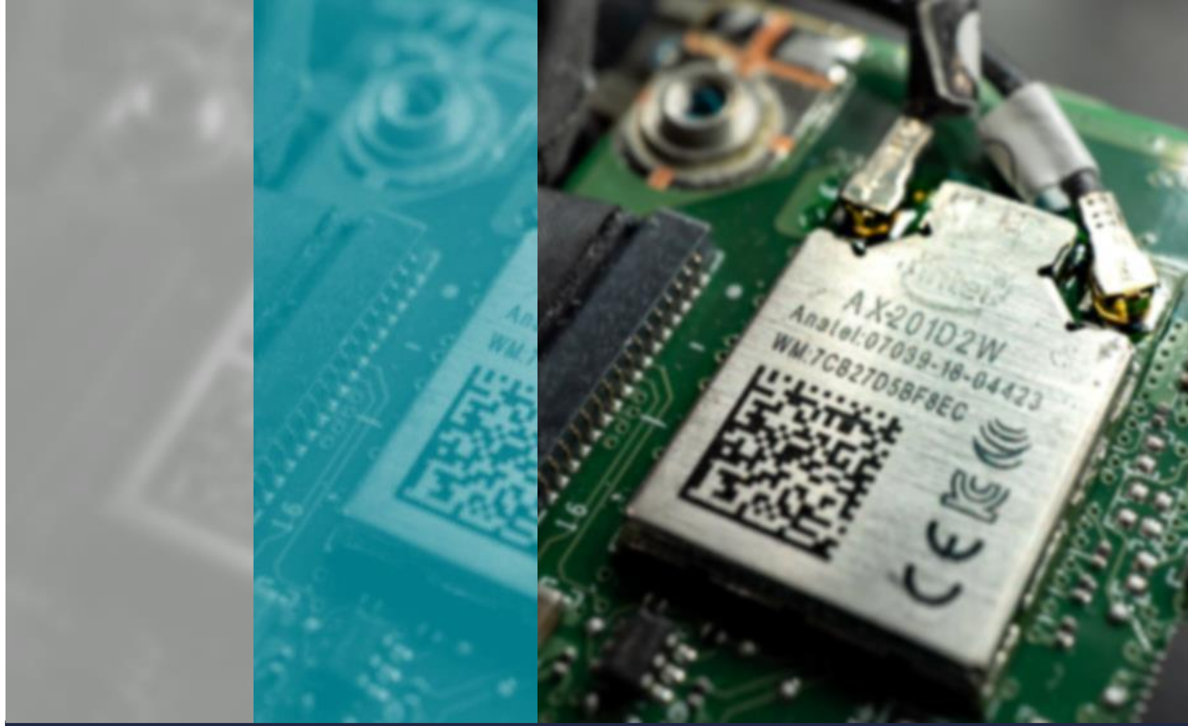
STATUS

- **RESOLVED**

RESOLUTION

- Intel recommends updating the Intel® ProSet/Wireless WiFi drivers to version 22.0 or later.

  Updates are available for download at this location:
  https://downloadcenter.intel.com/download/30208



Intel® ProSet/Wireless WiFi Driver Advisory

[Intel-SA-00472]

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- A potential security vulnerability in some Intel Atom® Processors may allow information disclosure. Intel is releasing firmware updates to mitigate this potential vulnerability.

- **Vulnerability Details:**

  CVEID: CVE-2020-24513

  Description: Domain-bypass transient execution vulnerability in some Intel Atom(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

- **Affected Products:**

  A list of impacted products can be found here.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00465.html

STATUS

- **RESOLVED**

RESOLUTION

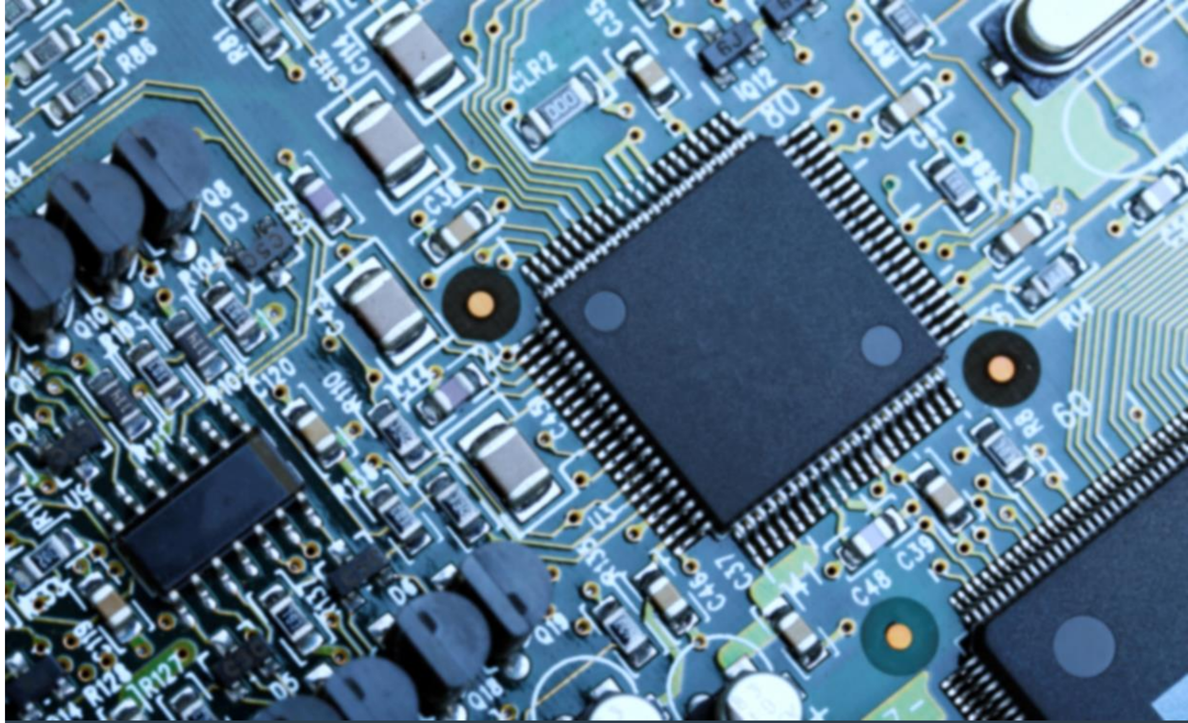
- Intel recommends that users of Intel® Processors update to the latest version provided by Dynabook Inc. that addresses these issues.

  To address this issue, an SGX TCB recovery is planned for Q2 2021. Customers will require the software update to get successful attestation responses. For customers using the Intel Attestation Service (IAS), the IAS Development Environment (DEV) will enforce the software updates beginning June 15, 2021 and the IAS Production Environment (LIV) will enforce the updates beginning July 13, 2021.

  For customers that are not using IAS, but instead are constructing their own attestation infrastructure using the Intel® SGX Provisioning Certificate Service (PCS), updated Endorsements/Reference Values (i.e., PCK Certificates and verification collateral) will be available June 8, 2021. These customers decide when to enforce the software update, as part of their Appraisal Policies.

  Refer to Intel® SGX Attestation Technical Details for more information on the SGX TCB recovery process.

  Further TCB Recovery Guidance for developers is available.



2021.1 IPU - Intel Atom® Processor Advisory

[Intel-SA-00465]

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- Potential security vulnerabilities in some Intel® Processors may allow information disclosure. Intel is releasing firmware updates to mitigate these potential vulnerabilities.

- **Vulnerability Details:**

  CVEID: CVE-2020-24511
  Description: Improper isolation of shared resources in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

  CVEID: CVE-2020-24512
  Description: Observable timing discrepancy in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

- **Affected Products:**

  A list of impacted products can be found here.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00464.html

STATUS

- **IN PROGRESS**

RESOLUTION

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

  Intel recommends that users of affected Intel® Processors update to the latest version firmware provided by dynabook Inc. that addresses this issue. Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available updates.

  Intel has released microcode updates for the affected Intel® Processors that are currently supported on the public github repository. Please see details below on access to the microcode:

  GitHub*: Public Github: https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files.

2021.1 IPU – Intel® Processor Advisory

[Intel-SA-00464]

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

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

- **Vulnerability Details:**

  CVEID: CVE-2020-12357
  CVEID: CVE-2020-8670
  CVEID: CVE-2020-8700
  CVEID: CVE-2020-12359
  CVEID: CVE-2020-12358
  CVEID: CVE-2021-0095
  CVEID: CVE-2020-12360
  CVEID: CVE-2020-24486

- **Affected Products:**

  For a complete list of affected products, please see Intel Security Advisory page.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00463.html

STATUS

- **IN PROGRESS**

RESOLUTION

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

  Intel recommends that users of the affected products update to the latest firmware version provided by dynabook Inc. that addresses this issue. Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available updates.

2021.1 IPU – BIOS Advisory

[Intel-SA-00463]

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- Potential security vulnerabilities in the Intel® Converged Security and Manageability Engine (CSME), Server Platform Services (SPS), and Intel® Local Manageability Service (Intel® LMS) may allow escalation of privilege or information disclosure. Intel is releasing firmware and software updates to mitigate these potential vulnerabilities.

- **Vulnerability Details:**

  CVEID: CVE-2020-24509
  CVEID: CVE-2020-8704
  CVEID: CVE-2020-24507
  CVEID: CVE-2020-24516
  CVEID: CVE-2020-8703
  CVEID: CVE-2020-24506

- **Affected Products:**

  For a complete list of affected products, please see Intel Security Advisory page.

  Note: Firmware versions of Intel® ME 3.x thru 10.x, Intel® TXE 1.x thru 2.x, and Intel® Server Platform Services 1.x thru 2.X are no longer supported versions. There is no new general release planned for these versions.

- **Intel® security center advisory:**

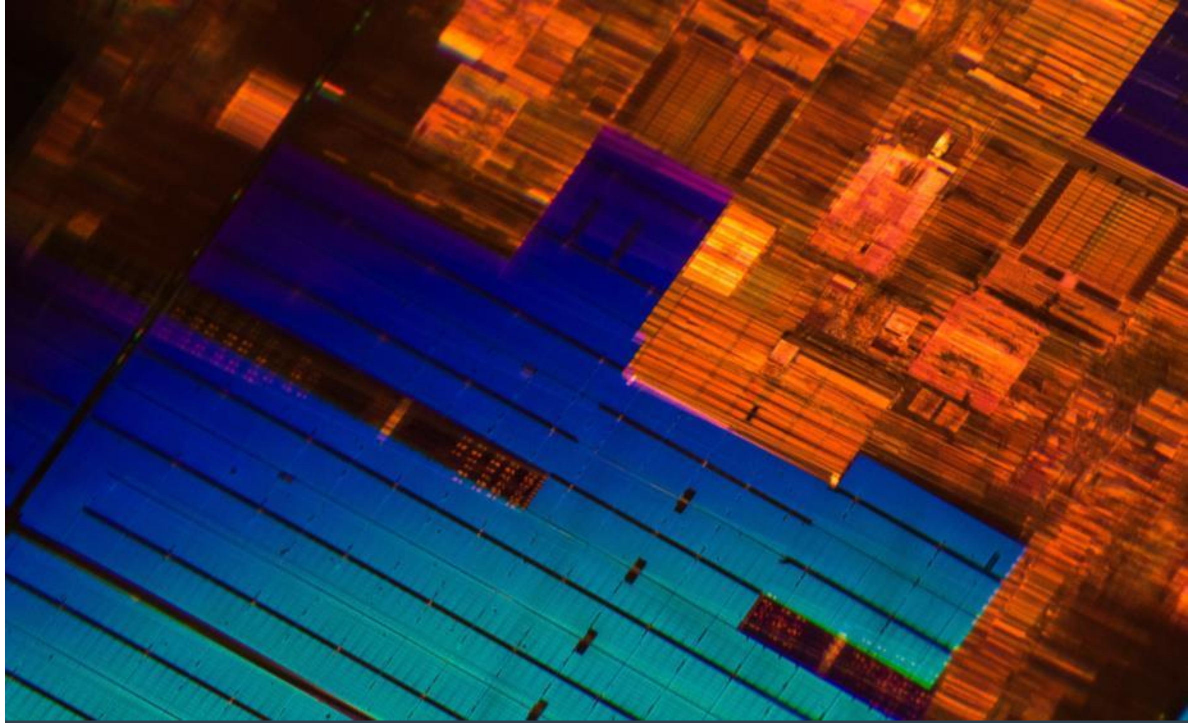
  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00459.html

STATUS

- **IN PROGRESS**

RESOLUTION

- Intel recommends that users of Intel® CSME, SPS and Intel® LMS update to the latest version firmware provided by the dynabook Inc. that addresses these issues. Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available updates.



2021.1 IPU – Intel® CSME, SPS and LMS Advisory

[Intel-SA-00459]

© 2021 Dynabook Europe GmbH

dynabook

VULNERABILTY SUMMARY

- A potential security vulnerability in the Intel® Software Guard Extensions (SGX) may allow information disclosure. Intel released firmware updates to mitigate this potential

- **Vulnerability Details:**

  CVEID: CVE-2020-24491

  Description: Debug message containing addresses of memory transactions in some Intel(R) 10th Generation Core Processors supporting SGX may allow a privileged user to potentially enable information disclosure via local access.

- **Affected Products:**

  10th Generation Intel® Core™ Processors supporting SGX.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00455.html

STATUS

- **IN PROGRESS**

RESOLUTION

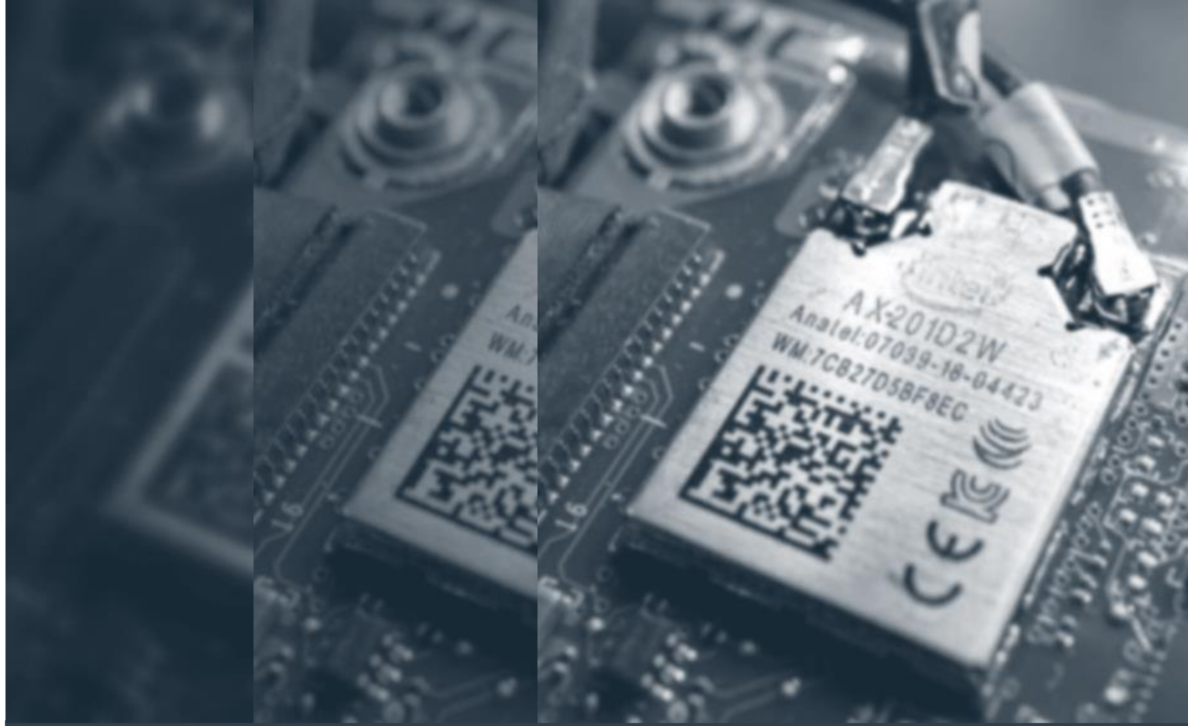
- Dynabook Inc. continues to work with Intel on updates with new versions available per guidance from Intel's Security Issue Update.

  Intel recommends that users of affected Intel® Processors update to the latest firmware version provided by dynabook Inc. that addresses this issue. Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available packages.

Intel® SGX Platform Advisory

[**Intel-SA-00455**]

© 2021 Dynabook Europe GmbH



Intel® PROSet/Wireless WiFi and Killer™ Driver Advisory

[Intel-SA-00448]

VULNERABILTY SUMMARY

- A potential security vulnerability in some Intel® PROSet/Wireless WiFi and Killer™ drivers for Windows 10* may allow information disclosure or denial of service. Intel is releasing software updates to mitigate this potential vulnerability.

- **Vulnerability Details:**

  CVEID: CVE-2020-24458

  Description: Incomplete cleanup in some Intel(R) PROSet/Wireless WiFi and Killer (TM) drivers before version 22.0 may allow a privileged user to potentially enable information disclosure and denial of service via adjacent access.

- **Affected Products:**

  Intel® PROSet/Wireless products: Intel® Wi-Fi 6 AX201 | AX200 | AC 9560 | AC 9462 | AC 9461
  Killer™ products: Killer™ Wi-Fi 6 AX1650 | AC 1550

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00448.html

STATUS

- **RESOLVED**

RESOLUTION

- Intel recommends updating the affected Intel® PROSet/Wireless and Killer™ driver (Netwtw10.sys) to version 22.00 or later. Updates for Intel® PROSet/Wireless drivers with Windows 10 are available for download at this location: https://www.intel.com/content/www/us/en/support.html.

  Customers can also download the latest available software from the Intel Customer Support site here.

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- A potential security vulnerability in some Intel® Virtualization Technology for Directed I/0 (VT-d) products may allow escalation of privilege. Intel is releasing firmware updates to mitigate this potential vulnerability.

- **Vulnerability Details:**

  CVEID: CVE-2020-24489

  Description: Incomplete cleanup in some Intel(R) VT-d products may allow an authenticated user to potentially enable escalation of privilege via local access.

- **Affected Products:**

  10th and 11th Generation Intel® Core™ Processors
  Intel® Pentium® Processor J Series, N Series
  Intel® Celeron® Processor J Series, N Series
  Intel® Atom® Processor A Series, E3900 Series
  Intel® Pentium® Processor Silver Series/ J&N Series
  Intel® Pentium® Processor Silver Series/ J&N – Refresh
  Intel® Core™ Processors with Intel® Hybrid Technology

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00442.html

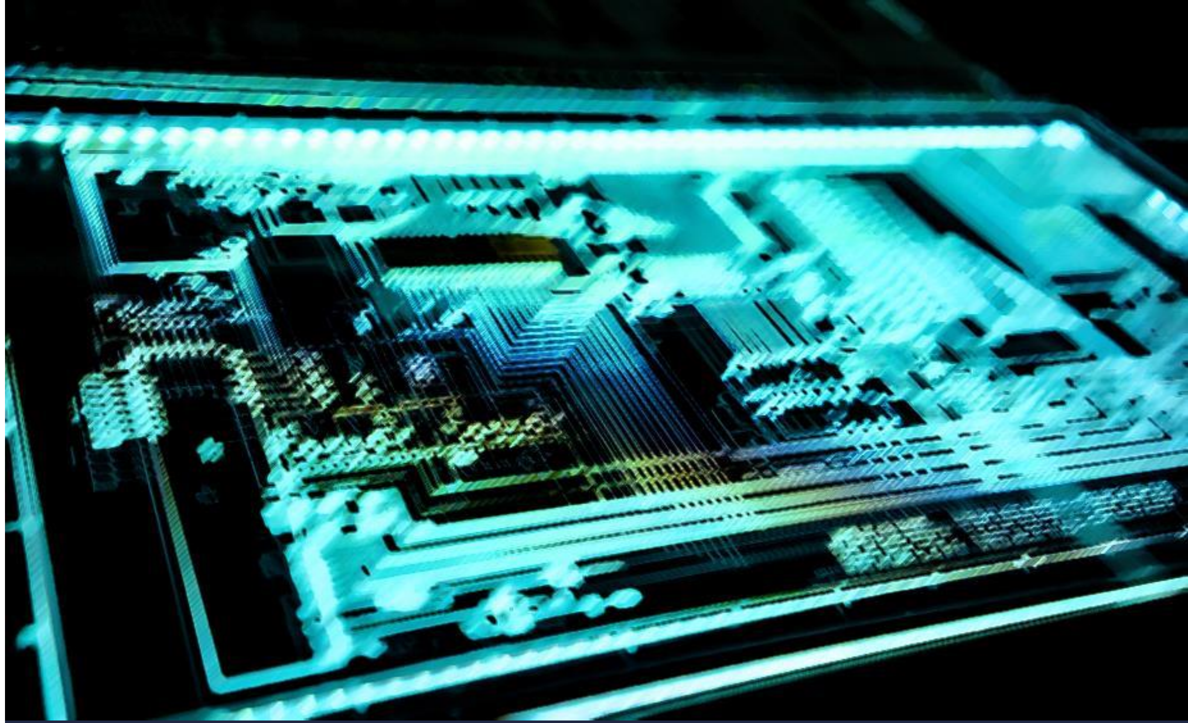
STATUS

- **IN PROGRESS**

RESOLUTION

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

  Intel recommends that users of Intel® VT-d update to the latest firmware version provided by dynabook Inc. that addresses this issue. Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available packages.



2021.1 IPU - Intel® VT-d Advisory

[**Intel-SA-00442**]

© 2021 Dynabook Europe GmbH

dynabook

VULNERABILTY SUMMARY

- Potential security vulnerabilities in some 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-2020-0544 | CVEID: CVE-2020-0521 | CVEID: CVE-2020-12362
  CVEID: CVE-2020-12361 | CVEID: CVE-2020-24450 | CVEID: CVE-2020-24462
  CVEID: CVE-2020-8678 | CVEID: CVE-2020-0518 | CVEID: CVE-2020-12367
  CVEID: CVE-2020-12368 | CVEID: CVE-2020-12369 | CVEID: CVE-2020-12385
  CVEID: CVE-2020-12365 | CVEID: CVE-2020-12366 | CVEID: CVE-2020-24448
  CVEID: CVE-2020-12386 | CVEID: CVE-2020-12384 | CVEID: CVE-2020-12363
  CVEID: CVE-2020-12364 | CVEID: CVE-2020-12370 | CVEID: CVE-2020-12371
  CVEID: CVE-2020-12372 | CVEID: CVE-2020-12373

- **Affected Products:**

  Intel® Graphics Drivers for 3rd, 4th, 5th, 6th, 7th, 8th, 9th and 10th Generation Intel® Processors for Windows* 7, 8.1 and 10 before versions 15.33.51.5146, 15.36.39.5145, 15.40.46.5144, 15.45.32.5164, 26.20.100.8141, 27.20.100.8587 and Intel® Graphics Drivers for Linux before Linux kernel version 5.5.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00438.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.

  Please visit http://emea.dynabook.com/support/drivers/laptops/ for download the latest Intel® Graphics Driver published by Dynabook Inc or check Microsoft® Windows Update function to obtain available packages.

Intel® Graphics Drivers Advisory

[Intel-SA-00438]

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- Potential security vulnerability in Intel® Active Management Technology (AMT), and Intel® Standard Manageability (ISM) may allow escalation of privilege. Intel is releasing firmware updates to mitigate this potential vulnerability.

- **Vulnerability Details:**

  CVEID: CVE-2020-8758

  Description: Improper buffer restrictions in network subsystem in provisioned Intel(R) AMT and Intel(R) ISM versions before 11.8.79, 11.12.79, 11.22.79, 12.0.68 and 14.0.39 may allow an unauthenticated user to potentially enable escalation of privilege via network access. On un-provisioned systems, an authenticated user may potentially enable escalation of privilege via local access.

- **Affected Products:**

  Intel® AMT and Intel® ISM versions before 11.8.79, 11.12.79, 11.22.79, 12.0.68 and 14.0.39.

  The following CVE assigned by Intel, corresponds to a CVE disclosed on 12/18/2020 as part of ICSA-20-353-01: Disclosed in INTEL-SA-00404 / Disclosed in ICSA-20-353-01 -CVE-2020-8758 / CVE-2020-25066

  Note: Firmware versions of Intel® ME 3.x thru 10.x, Intel® TXE 1.x thru 2.x, and Intel® Server Platform Services 1.x thru 2.X are no longer supported versions. There is no new general release planned for these versions.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00404.html

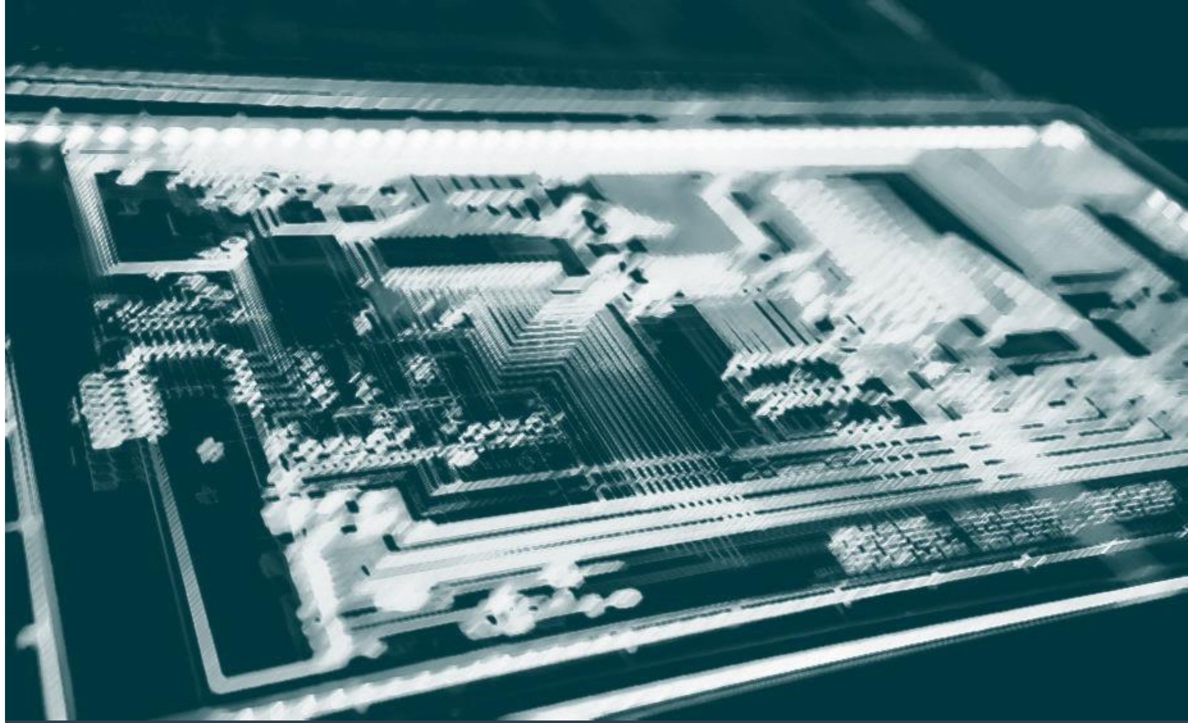
STATUS

- **RESOLVED**

RESOLUTION

- Intel recommends that users of Intel® AMT and Intel® ISM update to the latest version provided by dynabook Inc. that addresses these issues.

  Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available packages.



Intel® AMT and Intel® ISM Advisory

[Intel-SA-00404]

© 2021 Dynabook Europe GmbH

dynabook

VULNERABILTY SUMMARY

- Potential security vulnerabilities in some Intel® Thunderbolt™ controllers may allow denial of service. Intel is releasing firmware updates to mitigate these potential vulnerabilities..

- **Vulnerability Details:**

  Please refer to the Intel security center advisory (link below) for details.

- **Affected Products:**

Retimer and USB Retimer	Before Version
Intel® DSL5520	All
Intel® DSL5320	All
Intel® DSL6340	All
Intel® DSL6540	All
Intel® JHL6540	46
Intel® JHL6340	46
Intel® JHL6240	21
Intel® JHL7540	60
Intel® JHL7340	60
Intel® JHL7440	60
Intel® JHL8040R	41
Intel® JHL8010R	41

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00401.html

STATUS

- **RESOLVED**

RESOLUTION

- Intel recommends that users of Intel® Thunderbolt™ controllers update to the latest version provided by Dynabook Inc. that addresses these issues.

  Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available packages.

Intel® Thunderbolt™ Controller Advisory

[Intel-SA-00401]

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- A potential security vulnerability in the Intel® Thunderbolt™ non-DCH (Declarative Componentized Hardware) driver for Windows may allow escalation of privilege. Intel is releasing software updates and prescriptive guidance to mitigate this potential vulnerability.

- **Vulnerability Details:**

  CVEID: CVE-2020-8741

  Description: Improper permissions in the installer for the Intel(R) Thunderbolt(TM) non-DCH driver, all versions, for Windows may allow an authenticated user to potentially enable escalation of privilege via local access.

- **Affected Products:**

  Intel® Thunderbolt™ non-DCH Driver, all versions, for Windows..

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00393.html

STATUS

- **RESOLVED**

RESOLUTION

- Intel has issued a Product Discontinuation notice for the Intel® Thunderbolt™ non-DCH driver for Windows. To retain support for existing devices, Intel recommends that users of Intel® Thunderbolt™ non-DCH driver for Windows update to the latest version provided by Dynabook Inc.

  Please visit http://emea.dynabook.com/support/drivers/laptops/ to download the latest Intel® non-DCH driver for Windows published by Dynabook Inc or check Microsoft® Windows Update function to obtain available packages.

Intel® Thunderbolt™ non-DCH Driver for Windows Advisory

[**Intel-SA-00393**]

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

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

  Intel is not releasing updates to mitigate a potential vulnerability and has issued a Product Discontinuation Notice for Intel® DAL SDK.

- **Vulnerability Details:**

  Please refer to the Intel security center advisory (link below) for details.

- **Affected Products:**

  Intel® CSME and Intel® AMT versions before 11.8.82, 11.12.82, 11.22.82, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25. Intel® TXE versions before 3.1.80 and 4.0.30.
  The following CVEs assigned by Intel, correspond to a subset of the CVEs disclosed on 12/18/2020 as part of ICSA-20-353-01:
  Disclosed in INTEL-SA-00391: CVE-2020-8752 / CVE-2020-8753 / CVE-2020-8754
  Disclosed in ICSA-20-353-01: CVE-2020-27337 / CVE-2020-27338 / CVE-2020-27336

  Note: Firmware versions of Intel® ME 3.x thru 10.x, Intel® TXE 1.x thru 2.x, and Intel® Server Platform Services 1.x thru 2.X are no longer supported versions. There is no new general release planned for these versions.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00391.html

STATUS

- **RESOLVED**

RESOLUTION

- Intel recommends that users of Intel® CSME, Intel® TXE, Intel® AMT and Intel® SPS update to the latest version provided by Dynabook Inc. that addresses these issues.
  The Intel® AMT SDK is available for download here.

  Intel has issued a Product Discontinuation notice for the Intel® DAL SDK and recommends that users of the Intel® DAL SDK uninstall it or discontinue use at their earliest convenience.

  Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available packages.

2020.2 IPU – Intel® CSME, SPS, TXE, and AMT Advisory

[Intel-SA-00391]

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- Potential security vulnerabilities in the Intel® Running Average Power Limit (RAPL) Interface may allow information disclosure. Intel is releasing microcode and Linux driver updates to mitigate these potential vulnerabilities.

- **Vulnerability Details:**

  CVEID: CVE-2020-8694
  Description: Insufficient access control in the Linux kernel driver for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

  CVEID: CVE-2020-8695
  Description: Observable discrepancy in the RAPL interface for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.

- **Affected Products:**

  For a complete list of affected products, please see below link to Intel® security center advisory.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00389.html

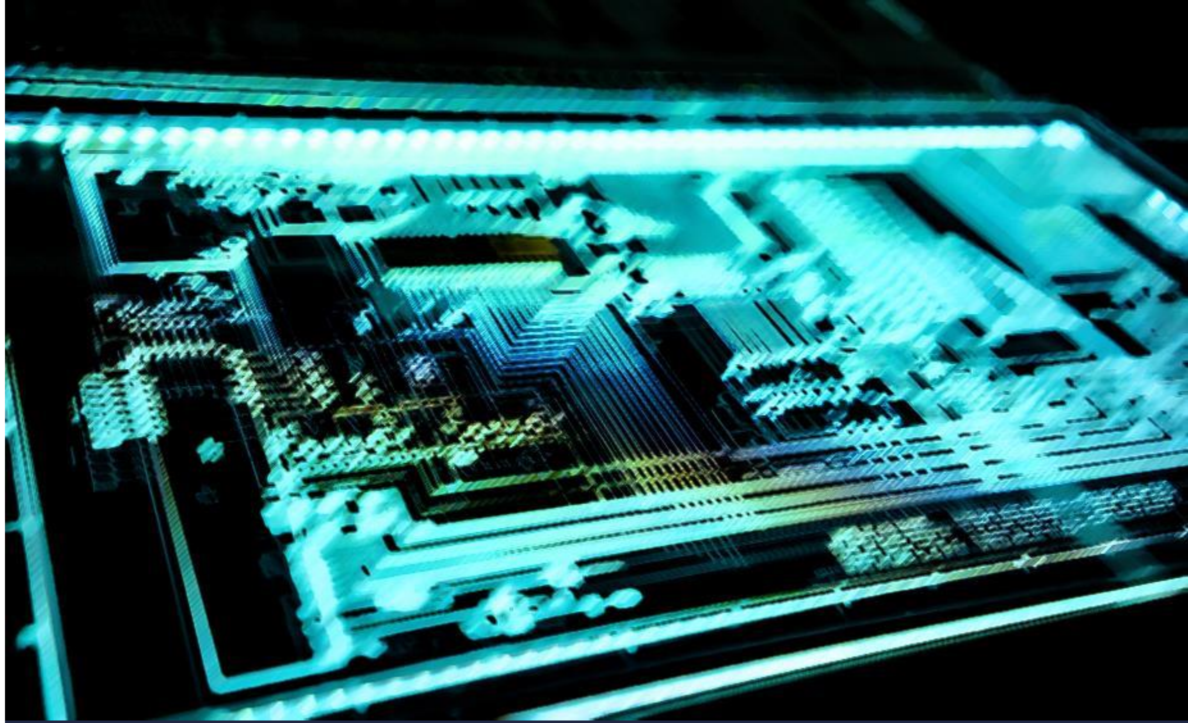
STATUS

- **IN PROGRESS**

RESOLUTION

- Intel recommends that users of affected Intel® Processors update to the latest firmware version provided by dynabook Inc. that addresses this issue. Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available packages.

  Intel recommends that users of affected Intel® Processors install the updates provided by their software vendors. In Linux, for the change to be effective it will require a reboot. If a reboot is not possible, Intel recommends changing the permissions of the affected sysfs attributes so that only privileged users can access them.



2020.2 IPU - Intel® RAPL Interface Advisory

[**Intel-SA-00389**]

© 2021 Dynabook Europe GmbH

VULNERABILTY SUMMARY

- Potential security vulnerabilities in some Intel® Processors may allow information disclosure. Intel is releasing firmware updates to mitigate these potential vulnerabilities.

- **Vulnerability Details:**

  CVEID: CVE-2020-8698
  Description: Improper isolation of shared resources in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

  CVEID: CVE-2020-8696
  Description: Improper removal of sensitive information before storage or transfer in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

- **Affected Products:**

  A list of impacted products can be found here.

- **Intel® security center advisory:**

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00381.html

STATUS

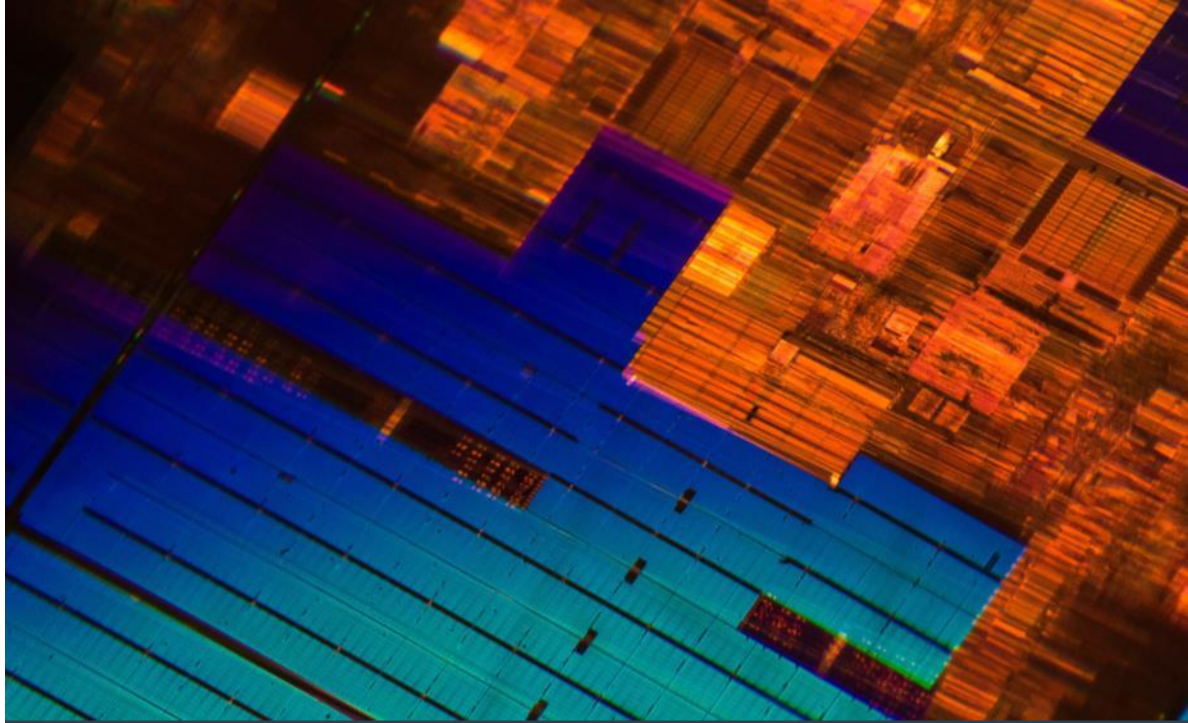
- **RESOLVED**

RESOLUTION

- Intel recommends that users of affected Intel® Processors update to the latest version firmware provided by the dynabook Inc. that addresses these issues. Please visit and check http://emea.dynabook.com/support/drivers/laptops/ for available BIOS updates.

  Intel has released microcode updates for the affected Intel® Processors that are currently supported on the public github repository. Please see details below on access to the microcode:
  GitHub*: Public Github: https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files

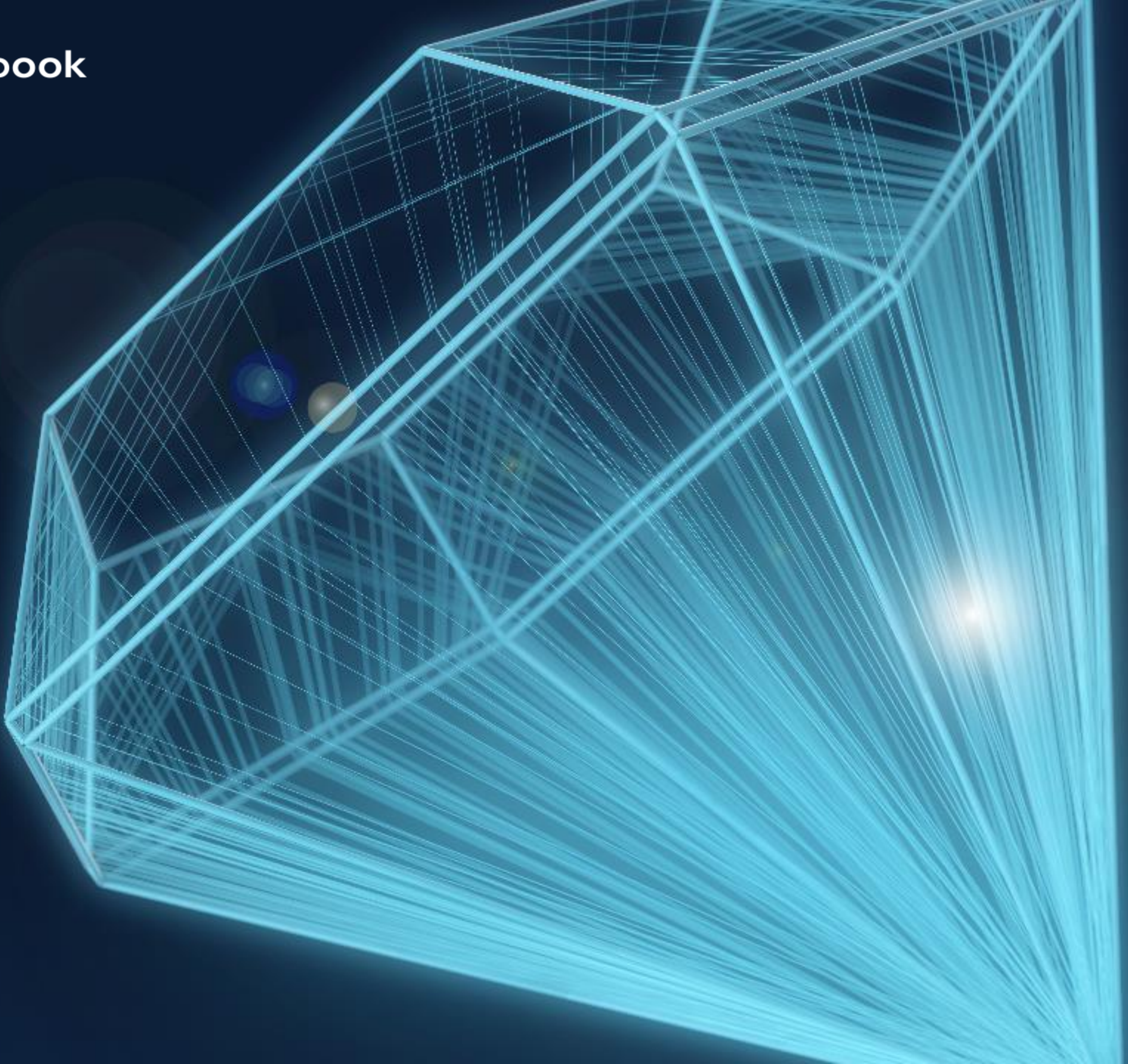
  To address this issue, an SGX TCB recovery will be required in Q4 2020. Refer to Intel® SGX Attestation Technical Details for more information on the SGX TCB recovery process.



2020.2 IPU - Intel® Processor Advisory

[Intel-SA-00381]

© 2021 Dynabook Europe GmbH



© 2021 Dynabook Europe GmbH