



PRODUCTS: NUC12SNKI7

Version 0060 - SNADL357.0060.2024.0227.1358

About This Release:

- ROM Image Checksum: 0x95264626
- EC Firmware: 01.17.00
- ME Firmware: 16.1.30.2307
- PCH Configuration Firmware: 16.1.0.1014
- PMC Firmware: 160.1.0.1030
- iTBT Firmware: 16.0.0.0202
- IOM Firmware: IOM_24.0006.0.0_prod
- NPHY Firmware: 14.531.509.8259
- Platform Properties Assessment Module:
- CRB Label: 5.26_1AXFE_RCOC.00.71.76(3275.00)_054
- Boot Guard ACM: 1.18.10
- Bios Guard: 2.0.5021
- Silicon Initialization Code: 0C.00.71.76(3275.00)
- Memory Reference Code: 0.0.4.36
- Integrated Graphics GOP
 - UEFI Driver: 21.0.1054
- Intel RST Pre-OS:
 - VMD UEFI Driver: 19.5.0.5676
- AHCI Code: AHCI_31
- Supported Flash Devices:
 - WinBond W25Q256JV 32MB
 - GD25R256E 32MB
 - GD25R256D 32MB
- Microcode Updates included in .BIN & .CAP Files:
 - M80906A3_00000432.pdb

Security Patch:

1. NetworkPkg EDK2
2. Flash driver security review
3. 2024.1 Intel Platform Update
4. 2023.4 Intel Platform Update
5. UsbRt TOCTOU Vulnerability
6. Image Parser Corruption Vulnerability
7. UsbSmmRt vulnerability
8. LogoFAIL Vulnerability

Feature Change/Update:

1. Update ME to 16.1.30.2307
2. Update MCU to 0x432

Issue Fix:

1. When "USB S4/S5 Power" set to "Disabled", still can wake up from USB S5 power
2. If use F7 update that not support BIOS revision .CAP file, the message have "Intel" link
3. cannot do WU update from current BIOS version to next BIOS version
4. Update Intel KEK/DB keys to support MSFT CA 2023

LEGAL INFORMATION

Information in this document is provided in connection with ASUS Products and for the purpose of supporting ASUS developed server/desktop boards and systems.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in ASUS's Terms and Conditions of Sale for such products, ASUS assumes no liability whatsoever, and ASUS disclaims any express or implied warranty, relating to sale and/or use of ASUS products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. ASUSTeK Computer Inc. may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights. ASUS products are not intended for use in medical, life saving, or life sustaining applications. ASUS may make changes to specifications and product descriptions at any time, without notice.

ASUS and the ASUS logo are trademarks of ASUSTeK Computer Incorporated.
Copyright © 2024, ASUSTeK Computer Inc. All rights reserved.