Hewitt Lake / Grangeville NS Platform

BIOS Release Notes

April 2022

Revision 12.D13

Notice: This document contains information on products in the design phase of development. The information here is subject to change without notice. Do not finalize a design with this information.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

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

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel® Turbo Boost Technology requires a PC with a processor with Intel Turbo Boost Technology capability. Intel Turbo Boost Technology performance varies depending on hardware, software and overall system configuration. Check with your PC manufacturer on whether your system delivers Intel Turbo Boost Technology. For more information, see http://www.intel.com/technology/turboboost

Warning: Altering PC clock or memory frequency and/or voltage may (i) reduce system stability and use life of the system, memory and processor; (ii) cause the processor and other system components to fail; (iii) cause reductions in system performance; (iv) cause additional heat or other damage; and (v) affect system data integrity. Intel assumes no responsibility that the memory, included if used with altered clock frequencies and/or voltages, will be fit for any particular purpose. Check with memory manufacturer for warranty and additional details.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

Cost reduction scenarios described are intended as examples of how a given Intel- based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

Intel® AMT should be used by a knowledgeable IT administrator and requires enabled systems, software, activation, and connection to a corporate network. Intel AMT functionality on mobile systems may be limited in some situations. Your results will depend on your specific implementation. Learn more by visiting Intel® Active Management Technology.

Intel is a sponsor and member of the Benchmark XPRT Development Community, and was the major developer of the XPRT family of benchmarks. Principled Technologies is the publisher of the XPRT family of benchmarks. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Contents

1 Disclaimer

Intel attempts to release Server BIOS binaries, under NDA for testing on supported CRBs that adhere to the same security requirements as should be used in production. However, some BIOS differences exist. The differences, which do not adhere to security requirements, that should be addressed before releasing a product based on for this release are listed below:

1. GPIO lock: The current CRB BIOS binary leaves the GPIOs unlocked, with a setup control to change the default. In a true production BIOS, the GPIOs are locked and no setup control to override exists.

2. SPI Lock: The current CRB BIOS binary leaves SPI unlocked to allow ease of upgrade in the field using non-production applications to upgrade CRBS to non-production binaries. In a true production BIOS, SPI is locked. In particular, the SPI flash descriptor permissions should be set to least privilege.

3. Runtime Variables: The current CRB BIOS binary defines Several PCDs as Dynamic HII PCDs such that validation has maximum flexibility in debug by offering setup control over these features. In a true production BIOS, these PCDs should be static PCDs configured at build time.

4. SWSMI Interface: The current CRB BIOS binary exposes several SWSMI functions to support ease of configuration by internal validation applications. The source code to these functions has not been included, though they are present in the binary. In a true production BIOS, these interfaces should not exist.

2 Potential issues

*Note: below table lists sightings that are under investigation

ID	Title
None	

3 BIOS Releases

*Note: this section lists fixed issues in each BIOS revision

3.1 BIOS revision: 12D13 (IPU 2022.2)

- b4592efe - [INTEL-UA-00365] Update memory/io allocation
- 6d3d5958 - GrantleyPkg\Ras\Whea: System got hangs after injecting uncorrectable error
- 7ccfe4fa - [BDX-DE NS] System got hangs after injecting uncorrectable error

3.2 BIOS revision: 12D08 (IPU 2022.1)

- ae81237f - [CVE-2021-0154] Possible SMRAM corruption in Memras
- 51519cbf - [CVE-2021-0154] Possible SMRAM corruption in Memras
- c61d55d5 - [CVE-2021-0155] Incorrect pointer validation in Memras
- a4fc616b - GrantleyRestrictedPkg\GrangevilleStitchingPkg\microcode: IPU2021.2_PV_Integrating microcode m1050665_0e000014

3.3 BIOS revision: 12D02 (IPU 2021.2)

- 490cce1e - GrantleyRestrictedPkg\GrangevilleStitchingPkg\microcode: IPU2021.2_Beta_Integrating microcode m1050665_0e000013
- 3d089d91 - GrantleyPkg: CVE-2020-8673 changes and support for opt out
- 65d3ebb6 - GrantleyPkg: CVE-2020-8673 changes and support for opt out
- b7492eb1 - Potential arbitrary code execution during the Pre-Efi Initialization (PEI) stage
- a1f46582 - OpenSSL update to 1.1.1j
- 3eb7a056 - GrantleyPkg: Support Core Bios Done in BIOS
- b1802c2c - IPU2021.1_Beta_Integrating microcode m1050665_0e000012
- ce98fd6d - Migration from Perforce //CP_Server_Bios/Grangeville_NS to Git GrangevilleNS

3.4 BIOS revision: 11D08 (IPU 2021.1)

- 660518:Integrating microcode- m1050665_0e000011
- 659571:BUMP UP reference code version to BDX-DE 02.09.00.00 No
- 659570:1508466793: SUT will hang DXE assert after connecting LPC TPM 2.0. Fix: Link the correct PcdLib to the driver
- 659564:22010398935: [CVE-2020-12357] FW-UEFI-Vuln-2020-006 SMM-module - MemRas - Missing pointer validation
- 659532:14012023084: [CVE-2020-12360] SMI 0x9a mEinjParam address is not correctly passed to OS

3.5 BIOS revision: 11D02 (IPU 2020.2)

- 655188:ipu2020.2-beta- Integrating SPS_SoC-X_03.00.03.100.0_PC-GVL_REL
- 654004:14011449175: FW-UEFI-Vuln-2020-011 [PS]TPM Platform Auth Security Vulnerability
- 653415:BUMP UP reference code version to BDX-DE 02.08.00.00
- 653287:22010398982: FW-UEFI-Vuln-2019-183 [RC] SMM accessing memory outside of SMRAM and not validating the memory
- 653156:22010398982: FW-UEFI-Vuln-2019-183 [RC] SMM accessing memory outside of SMRAM and not validating the memory
- 653093: part 2: Add latest inf to CryptoPkg.dsc Import dso_conf.h, opemsslconf.h, CrtLibSupport.h from EDK2
- 653091:HSDESID: part 1: Import Openssl folder from EDK2 on 21/04/2020 Along with OpensslLib.inf, OpensslLib.uni, buildinf.h, process_files.pl, OpenSSL-HOWTO.txt and some additional files in the OpensslLib folder
- 652672:Update Copyright for files committed by @652088 22010398967: FW-UEFI-Vuln-2019-182 [PS] Out of Bounds memory writes. No
- 652393:22010398974 FW-UEFI-Vuln-2019-181 [RC] Decompress needs to be updated
- 652088:22010398967: FW-UEFI-Vuln-2019-182 [PS] Out of Bounds memory writes. This said code is not called in Grangeville as of now. masked by GRANGEVILLE_PLATFORM_ENABLE flag. But the mitigation is added
- 652084:22010398963: FW-UEFI-Vuln-2019-132 Unsecure write to SMRAM because of missing buffer validation

3.6 BIOS revision: 10D96 (WW52 BKC)

- 646702:1609105945:FW-UEFI-Vuln-2018-031 - Dynamic loops accessing one element beyond boundary due to <= operator
- 644472:PLR2-microcode-m1050665_0e00000f.inc
- 639998:Back out changelist 625219 Fix not needed because the SPS team didn't fix it on their side for this trunk.

3.7 BIOS revision: 10D92 (WW29 BKC)

- 638321:BUMP UP reference code version to BDX-DE 02.07.00.00
- 638308:1409405608:The Hewitt Lake (Grangeville NS) CPU RC problem. Port the work around from Purley BIOS #5370795.
- 638302:1409186294: TianoCore Security Issue 1136
- 638300:1507065882: Hewittlake: In SMBIOS Type 17 Structure - Memory Device Form factor showing wrong information 1607150096:[GNS-HWL] 16Gbit RDIMM Size and speed info is mismatch in OS dmidecode
- 637991:1607104407: Support 16Gb DIMM density DRAMs on Hewitt Lake CCB-1607121572: Enable 16Gb based DIMMs on Hewitt Lake

3.8 BIOS revision: 10D88 (WW24 BKC, Grangeville NS WW23 BKC)

- 636667:-microcode integration- m1050665_0e00000e-PV canididate
- 635567:updating new SPS-0x59 config XML files LPTCB_NM_MONO_CRB(0x13).xml and LPTCB_NM_MONO_INT(0x13).xml
- 635228:BUMP UP reference code version to BDX-DE 02.06.00.00
- 635227:Update Copyright for the recently committed files
- 635158:1607182858: PENN: Unhiding PCH Thermal device resulted in platform Denial of Service
- 635156:1607182871: PENN: Powerconfig test failed PIT not set
- 635155:1607182869: PENN: Powerconfig test failed FLEX_RATIO lock not set 1607182851: PENN: Powerconfig test failed -TDP LOCK not set 1607182865: PENN: Powerconfig test failed TURBO_ACTIVATION Lock not set 1607182853: PENN: PPIN Control lock test failed
- 635051:1607182834: PENN: Power management initialization configuration lock failed
- 634981:BDX-NS/Hewittlake microcode -m1050665_0e00000d - This is the official production release for Hewittlake PRQ.
- Modified for release
- 633560:Update SPS ME FW to SPS_SoC-X_03.00.03.059.0 in BIOS builds-PV candidate
- 632685:1607052773: Fix vulnarability CVE-2019-1543 on OpenSSL 1.1.0j library.

3.9 BIOS revision: 10D82 (WW17 BKC)

- 632685:1607052773: Fix vulnarability CVE-2019-1543 on OpenSSL 1.1.0j library.

3.10 BIOS revision: 10D78 (Initial release, WW11 BKC)

- 630159:1607052773: Migrate OpenSSL version to 1.1.0j - Part 1
- 629732:1607052773: Add OpenSSL 1.1.0j library. This is only for adding library. Code changes to use this library will be added later.
- 628511:1606938861: When CPU autonomous Cstate to Enable, board is stuck at Post code ?bf?
- 626456:NO_HSD: Update copyright date in BIOS setup browser UI APP
- 626432:updated microcode_DE.inf ,microcodeinternal_DE.inf,processorstartoem.asm and project map for m1050665_0e00000c.inc for BDW-DE NS(Grangville-NS)
- 625802:NO_HSD: Import the LT configuration lock changes from Grangeville_Trunk.
- 625763:NO_HSD: Import the PCH security settings for the GPIO lockdown.
- 625673:NO_HSD: Code alignment from the Grangeville_Trunk codebase.

- 625219:1806832928: CoreBiosDone HECI message functionality (Grantley, Grangeville)
- 625206:NO_HSD: Importing the BIOS build link error fix from the Grangeville_Trunk as is.
- 625202:[Update SPS ME FW to SPS_SoC-X_03.00.03.045.0 in BIOS builds
- 625195:1606938861: [GNV-NS] Discrepancies found in the Processor Power Management (PpmInitialize) UEFI driver of Grangeville_NS trunk
- 625192:NO_HSD: Import the PCH/ME Security related changes from the Grangeville_Trunk.
- 625031:NO_HSD: Import the fixes from Grangeville_Trunk related to IPS 1209144523, 1209389424, and 1405473259

3.11 Grangeville-DE NS release history

3.11.1 BIOS revision: 10D52

- Update SPS ME FW to SPS_SoC-X_03.00.03.039.0 in BIOS builds - Masking the capability to disable CLKOUT_PEG_A

3.11.2 BIOS revision: 10D51

- 508218:5003554: [Addendum] BDX-DE: BIOS should not allow for modifying PEG_A via ICC_SET_CLOCK_ENABLES HECI message (merge from Grangeville-DE stream)
- 508216:5003561: KlocWork Issue -- #5546:H:\GrantleySocketPkg\Library\MemoryQpiInit\Chip\Mem\MemAddrMap.c : 1133 (Adddendum to resolve the TC build failure #508091)
- 508091:Divide by zero exception may occur, if socketCount variable is zero
- 508075: Array out of bound exception for foundFail Array
- 508074: Array index out of bound exception for density index variable at line number 349.
- 508069: Array out of bound exception for baseIOTPhysicalAddress at line number 1387.
- 508063: Array out of bound exception might occur for dimmTypePresent' array.
- 508043: KlocWork Issue#5172: H:\GrantleyPkg\Ras\Smm\MemRas\MemRasRoutines.c:2565 | SystemAddressToDimmAddress()
- 508039: KlocWork Issue#8570::GrantleyPkg\Platform\Pei\PlatformInit\MemoryCallback.c:179 | InstallFvInfoPpi()
- 508038: KlocWork Issue#8241::GrantleyPkg\Me\AMT\Platform\Library\AmtPlatformLib\BdsMisc.c:271 | BdsLibRegisterNewOption()
- 508034: KlocWork Issue#6169::GrantleyPkg\Ras\Smm\MemRas\MemRasRoutines.c:2550 | SystemAddressToDimmAddress()

- 508026: KlocWork Issue#6965::GrantleyPkg\Platform\Dxe\Setup\SetupInfoRecords.c:394 | IdeCallback()
- 508022: KlocWork Issue#6220::GrantleyPkg\Cpu\Dxe\PlatformCpuPolicy\PlatformCpuPolicy.c:178 | PlatformCpuSmbiosData()
- 508014: KlocWork Issue#5738::GrantleyPkg\Ras\Smm\SmmErrorLog\MemoryErrorHandler.c:317 | DisableCSMI()
- 508008: KlocWork Issue#5530,GrantleyPkg\Platform\Dxe\PlatformIpmi\PlatformIpmi.c:130 | SendDimmInfoToBMC()
- 507996: KlocWork Issue#5365,GrantleyPkg\Legacy\Dxe\LegacyBiosPlatform\LegacyBiosPlatform.c:2070 | PlatformHooks()
- 507993: KlocWork Issue#4894::GrangevillePkg\Platform\Pei\PlatformInit\PlatformEarlyInit.c:502 | SendBiosIdToMcu()
- 507989: KlocWork Issue#4936,GrantleyPkg\Library\PlatformCapsuleLib\PlatformCapsuleLib.c:130 | ProcessCapsuleImage()
- 507984: Klockwork#5105, Array 'mIohInfo' of size 4 may use index value(s) 4..10
- 507946: Merging from DE
- 5003432: There is a S3 security issue in GrantleyRefresh code base.
- 507584: Merging from DE
- 507581: Merging from DE
- 507570: Merging from DE
- 5003550: Remove un-needed SPI Opcodes
- 507569: Merging from DE
- 5003554: BDX-DE: BIOS should not allow for modifying PEG_A via ICC_SET_CLOCK_ENABLES HECI message
- 507568: Merging from DE
- 5003548: BIOS needs to set non-legacy ADR flow option bit
- 507523: regDqSwz array has been used with out initialization at line number 3149. if we are using a array with out initialization,then there might be garbage value also.so we need to initialize array prior to using it.
- 507113:[5003564][Rev:2][Assigned][Please update SPS ME FW to SPS_SoC-X_03.00.03.036.0 in BIOS builds]
- 507083: Merging from DE
- 5003526: DDR3 and DDR4 Thermal Offset Tables are not correctly implemented in BIOS
- 507082: Merging
- 5003538: System IERR during warm reset after enable Fast Boot + WR CRC
- 506595:[NO-HSD] Debug Prints - Fixes / Enhancement
- 506582:5003465: [BDX DE NS] Chipsec failures on 10D07 BIOS
- 503661: Merging from DE
- [5003513]: [IPS 1209007434] Can not access to RTC/CMOS by MM command on EFI shell
- 503131: Merging from DE

- 5003467: TSV RDIMMs not booting on BDX-EP with BIOS Rev 3.7.0.
- 503117: Merging from DE
- [5003512]: [IPS 1208770931] System defining more than 16 flash parts will hang up with SPI Flash ID check failure - WITH FIX
- 502670:BDX-NS EGW A0 PRODUCTION patch 0x0e000004 Release - This is the official production release for BDX-NS PRQ.
- Pcode: Performance fix for latency reduction from IOSFSW Bridge to Odems validated. Request for change in POR.
- 501023: Merging from Grangeville_DE
- [5003459]: SB.SRIO.WMAA function wrongly implemented and not validated

3.11.3 BIOS revision: 10D43

- 495299:[5003551] Please update SPS ME FW to SPS_SoC-X_03.00.03.035.0 in BIOS builds]

3.11.4 BIOS revision: 10D41

- 491395:5003518: Requirement for Grangeville NS CRB BIOS to have it available to do knobs override on OS. Rollback //CP_Server_BIOS/Grangeville_NS/GrantleyPkg/Include/Guid/SetupVariable.h to revision 2; rollback CL 483973)
- 490048:5003544: [GVL-NS] BIOS main build script should have NS-specific ingredients
- (lprior to IFWI stitch process:- SPS ME FW set to latest v3.0.3.33, include the latest microcode patch in regular build, set ALLOW_DBG_UCODE_PATCH_IN_TXT to false, rollback submit #480363, enabled the latest NS production patch in miniBIOS builds)
- 483973:5003518: Requirement for Grangeville NS CRB BIOS to have it available to do knobs override on OS [temporary override to allow Si validation on CRB, this override will be removed for PV, or for any external release]
- 480930: Revert BuildImage.bat for previous version (Rev2) - For TXT issue fixed.
- 480363: Remove the previous WA for the debug patch to support production signed microcode.

3.11.5 BIOS revision: 10D36

- 466604: Integrated debug version microcode - m1050665_fe000002
- 480930: Revert BuildImage.bat for previous version (Rev2) - For TXT issue fixed.
- 480363: Remove the previous WA for the debug patch to support production signed microcode.
- 476562:5003534: [GNV-NS] Automated built IFWI images does not boot without ITP connected (First step: remove the ACMs and microcode code from old build scripts (FitGen) and rely only on IFWI stitch for integration)

3.11.6 BIOS revision: 10D31

- 466604: Integrated debug version microcode - m1050665_fe000002
- 5003528: Please update SPS ME FW to SPS_SoC-X_03.00.03.033.0 in BIOS builds
- 465846:[Build Script Enhancement]: Generate SPI IFWI image by excluding TXT/ACM
- 465337:[Klocwork ID4769.2891]: Pointer 'BitDesc' checked for NULL
- 465336:[Klocwork 4840]: Array 'QpiInternalGlobal->RtidBase[1]' of size 52 may use index value(s) 2..256
- 465333:5003510: BDx-DE NS Legacy CBDMA default selection change
- 451602:5003482: All MTRRs being used on large memory system
- 451595:5003486: Failures during warm reset testing DIMMs.
- 451593:5003468: Per socket based CompletionTimeout setup options incorrect
- 451590:5003470: Fast Boot Cold Enabled will cause BIOS hang during warm reboot
- 450752:5003499: Grangeville-NS v1.3.0 NPW ACM for integration into IFWI, Grangeville-NS SPS v3.0.3.27 for integration into IFWI
- 449006:5003498: it doesn't show the stepping of the silicon

3.11.7 BIOS revision: 10D22

- 443144:5003493: BDX-DE NS: WA for debug version Microcode
- 440457:5003491: [BDX DE NS] GbE1 2 Lan ports can't be switch off by setup knob.
- 439230:5003489: [BDX DE NS] NS uniphy recipe applys with DE V2's
- 435863: Add some debug messages for NS PO
- 434903:5003484: [BDX DE NS] integrate the NS PO patch m1050665_fe000001
- 434362:5003481: 2400 DIMM not supported on Echo Canyon and Camelback Mountain

A CBR BIOS errata

*Note: this section lists permanent errata for Intel CRB BIOS

ID	Description
None	