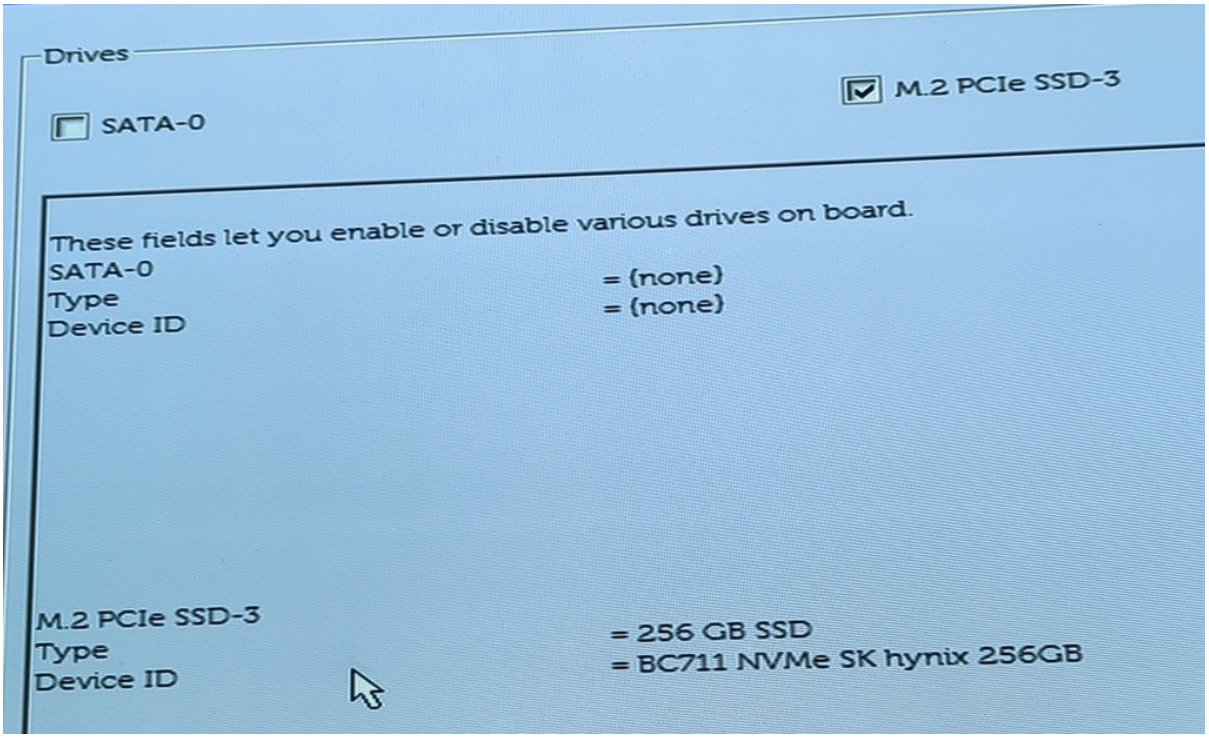
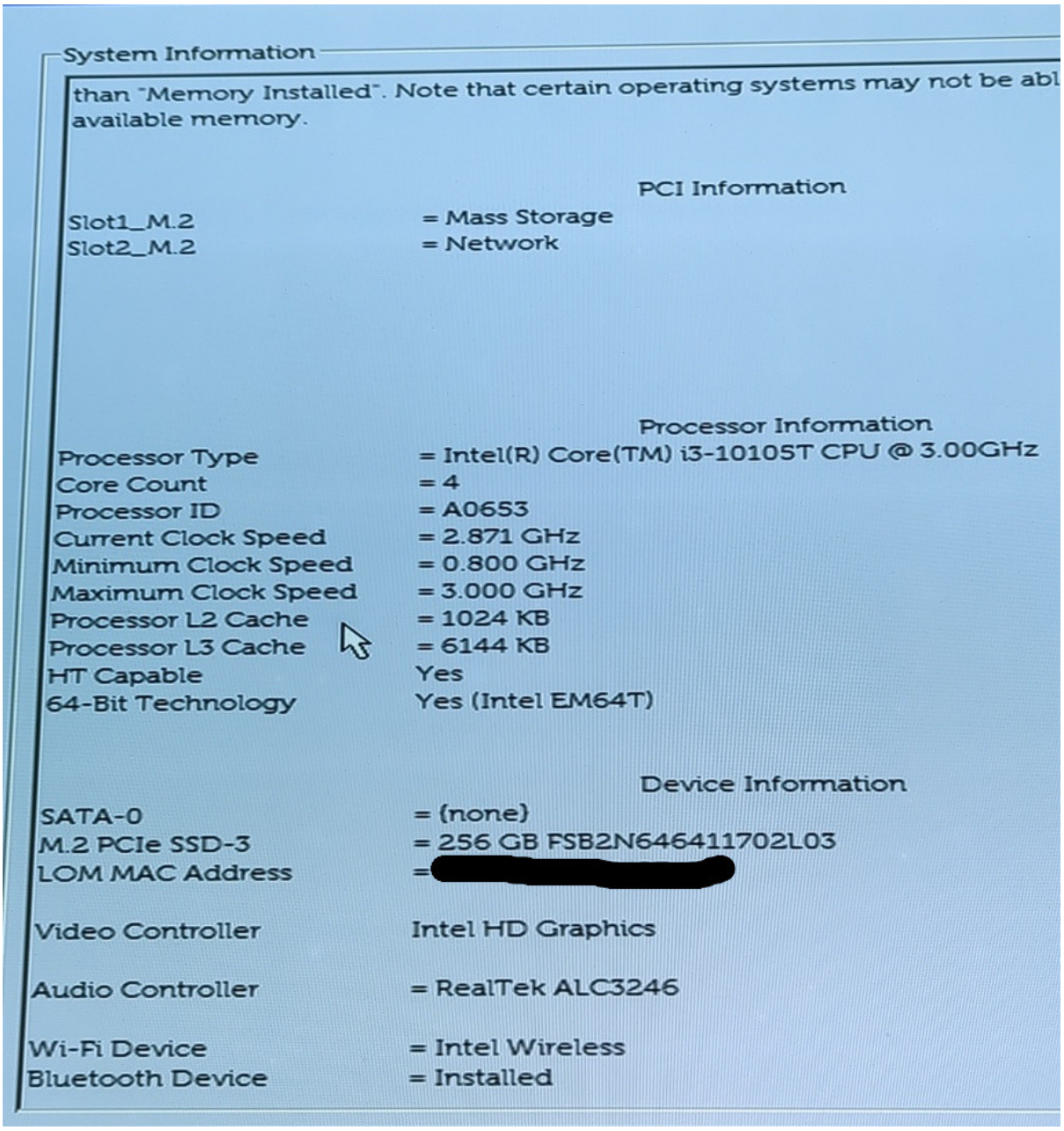
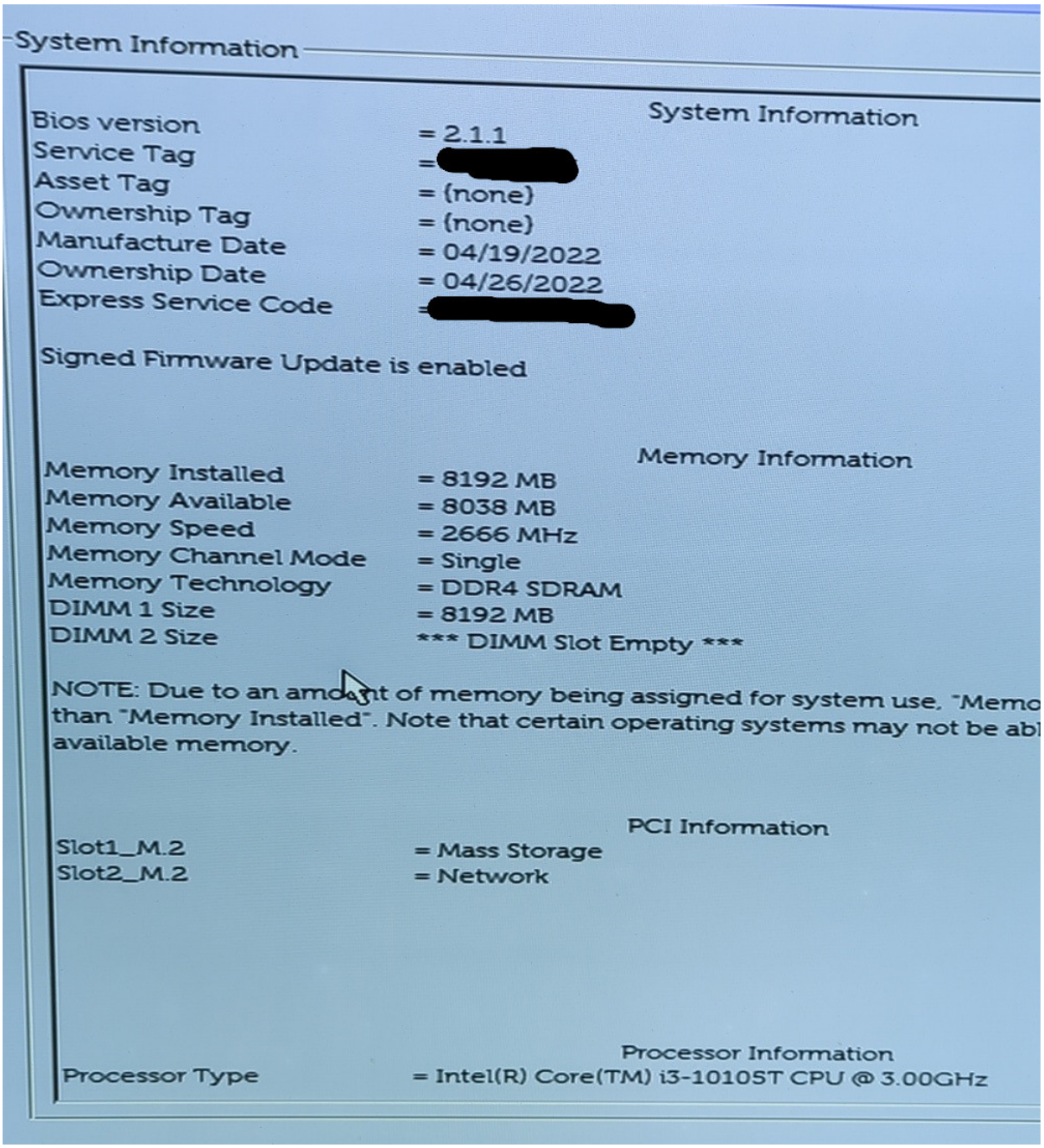
Ann

BIOS


Drives
SATA-0
M.2 PCIe SSD-3
These fields let you enable or disable various drives on board.
SATA-0
Type
Device ID
= (none)
= (none)
M.2 PCIe SSD-3
Type
Device ID
= 256 GB SSD
= BC711 NVMe SK hynix 256GB


System Information
than "Memory Installed". Note that certain operating systems may not be abl
available memory.
PCI Information
Slot1_M.2 = Mass Storage
Slot2_M.2 = Network
Processor Information
Processor Type = Intel(R) Core(TM) i3-10105T CPU @ 3.00GHz
Core Count = 4
Processor ID = A0653
Current Clock Speed = 2.871 GHz
Minimum Clock Speed = 0.800 GHz
Maximum Clock Speed = 3.000 GHz
Processor L2 Cache = 1024 KB
Processor L3 Cache = 6144 KB
HT Capable Yes
64-Bit Technology Yes (Intel EM64T)
Device Information
SATA-0 = (none)
M.2 PCIe SSD-3 = 256 GB FSB2N646411702L03
LOM MAC Address = [redacted]
Video Controller Intel HD Graphics
Audio Controller = RealTek ALC3246
Wi-Fi Device = Intel Wireless
Bluetooth Device = Installed



Hardware

RAM

- 1x 8GB 1Rx16 PC4-3200AA SOSIMM SK hynix
- DDR4-3200 (1600MHz) PC4-25600
- SODIMM DDR4 Synchronous 3200 MHz (0.3 ns)
- HMAA1GS6CJR6N-XN


SK hynix
CHINA
8GB 1Rx16 PC4 – 3200AA – SC0 – 13
HMAA1GS6CJR6N – XN N0 AC 2145
[redacted]
UK
CA
ECO

SSD


SK hynix
[redacted]
SSD(固態硬碟)
CAN ICES-3(B)/NMB-3(B)
BC711 NVMe SK hynix 256GB
S/N [redacted]
D P/N 0KFV6T WW : 2207
M/N(型號) : HFM256GD3GX013N BC
RATED(額定) : DC + 3.3V 2.5A
KR-0KFV6T-SK500-22L-0HFB-A03
R-R-HNX-BC711M230S
[redacted]
FW : 41002131
[redacted]
PSID : GRHZDACD F0000EGN
RLWS1448 C159222M
C
M.2 PCIe SSD-3
SATA-0

WiFi/BT

OS reported

```
    product: OptiPlex 3090 (0B8A)
    vendor: Dell Inc.
    serial: XXXX
    width: 64 bits
    capabilities: smbios-3.2.0 dmi-3.2.0 smp vsyscall32
    configuration: boot=normal chassis=desktop family=OptiPlex sku=0B8A uuid=XXX
  *-core
       description: Motherboard
       product: 02459H
       vendor: Dell Inc.
       physical id: 0
       version: A00
       serial: XXXX
     *-firmware
          description: BIOS
          vendor: Dell Inc.
          physical id: 0
```

```
          version: 2.1.1
          date: 12/13/2021
          size: 64KiB
          capacity: 32MiB
          capabilities: pci pnp upgrade shadowing cdboot bootselect edd int13floppy1200
int13floppy720 int13floppy2880 int5printscreen int9keyboard int14serial int17printer acpi usb
biosbootspecification netboot uefi
     *-memory
          description: System Memory
          physical id: 9
          slot: System board or motherboard
          size: 8GiB
        *-bank:0
             description: SODIMM DDR4 Synchronous 3200 MHz (0.3 ns)
             product: HMAA1GS6CJR6N-XN
             vendor: Hynix Semiconductor (Hyundai Electronics)
             physical id: 0
             serial: XXXX
             slot: DIMM1
             size: 8GiB
             width: 64 bits
             clock: 3200MHz (0.3ns)
        *-bank:1
             description: [empty]
             physical id: 1
             slot: DIMM2
     *-pci
          description: Host bridge
          product: 10th Gen Core Processor Host Bridge/DRAM Registers
          vendor: Intel Corporation
          physical id: 100
          bus info: pci@0000:00:00.0
          version: 03
          width: 32 bits
          clock: 33MHz
          configuration: driver=skl_uncore
          resources: irq:0
        *-display
             description: VGA compatible controller
             product: CometLake-S GT2 [UHD Graphics 630]
```

```
             vendor: Intel Corporation
             physical id: 2
             bus info: pci@0000:00:02.0
             version: 03
             width: 64 bits
             clock: 33MHz
             capabilities: pciexpress msi pm vga_controller bus_master cap_list rom
             configuration: driver=i915 latency=0
             resources: irq:135 memory:d0000000-d0ffffff memory:c0000000-cfffffff
ioport:4000(size=64) memory:c0000-dffff
        *-generic:0 UNCLAIMED
             description: System peripheral
             product: Xeon E3-1200 v5/v6 / E3-1500 v5 / 6th/7th/8th Gen Core Processor
Gaussian Mixture Model
             vendor: Intel Corporation
             physical id: 8
             bus info: pci@0000:00:08.0
             version: 00
             width: 64 bits
             clock: 33MHz
             capabilities: msi pm cap_list
             configuration: latency=0
             resources: memory:d1323000-d1323fff
        *-network
             description: Wireless interface
             product: Comet Lake PCH CNVi WiFi
             vendor: Intel Corporation
             physical id: 14.3
             bus info: pci@0000:00:14.3
             logical name: wlan0
             version: 00
             serial: c4:03:a8:e8:a7:79
             width: 64 bits
             clock: 33MHz
             capabilities: pm msi pciexpress msix bus_master cap_list ethernet physical
wireless
             configuration: broadcast=yes driver=iwlwifi driverversion=6.3.13_1
firmware=74.a5e9588b.0 QuZ-a0-hr-b0-74.u latency=0 link=no multicast=yes wireless=IEEE 802.11
             resources: irq:19 memory:d1314000-d1317fff
        *-pci:0
```

```
              description: PCI bridge
              product: Comet Lake PCI Express Root Port #17
              vendor: Intel Corporation
              physical id: 1b
              bus info: pci@0000:00:1b.0
              version: f0
              width: 32 bits
              clock: 33MHz
              capabilities: pci pciexpress msi pm normal_decode bus_master cap_list
              configuration: driver=pcieport
              resources: irq:122 memory:d1200000-d12fffff
            *-nvme
                 description: NVMe device
                 product: BC711 NVMe SK hynix 256GB
                 vendor: SK hynix
                 physical id: 0
                 bus info: pci@0000:01:00.0
                 logical name: /dev/nvme0
                 version: 41002131
                 serial: XXXX
                 width: 64 bits
                 clock: 33MHz
                 capabilities: nvme pm msi msix pciexpress nvm_express bus_master cap_list
                 configuration: driver=nvme latency=0 nqn=nqn.2022-02.com.skhynix:nvme:nvm-
subsystem-sn-XXXX state=live
                 resources: irq:16 memory:d1200000-d1203fff memory:d1205000-d1205fff
memory:d1204000-d1204fff
               *-namespace:0
                    description: NVMe disk
                    physical id: 0
                    logical name: hwmon0
               *-namespace:1
                    description: NVMe disk
                    physical id: 2
                    logical name: /dev/ng0n1
               *-namespace:2
                    description: NVMe disk
                    physical id: 1
                    bus info: nvme@0:1
                    logical name: /dev/nvme0n1
```

```
                  size: 238GiB (256GB)
                  capabilities: gpt-1.00 partitioned partitioned:gpt
                  configuration: guid=XXX logicalsectorsize=512 sectorsize=512 wwid=XXX
               *-volume
                    description: EFI partition
                    physical id: 1
                    bus info: nvme@0:1,1
                    logical name: /dev/nvme0n1p1
                    logical name: /mnt/nvme
                    serial: XXXX
                    capacity: 238GiB
                    configuration: mount.fstype=btrfs
mount.options=rw,relatime,ssd,discard=async,space_cache=v2,subvolid=5,subvol=/ state=mounted
        *-pci:1
             description: PCI bridge
             product: Intel Corporation
             vendor: Intel Corporation
             physical id: 1c
             bus info: pci@0000:00:1c.0
             version: f0
             width: 32 bits
             clock: 33MHz
             capabilities: pci pciexpress msi pm normal_decode bus_master cap_list
             configuration: driver=pcieport
             resources: irq:123 ioport:3000(size=4096) memory:d1100000-d11fffff
          *-network
               description: Ethernet interface
               product: RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller
               vendor: Realtek Semiconductor Co., Ltd.
               physical id: 0
               bus info: pci@0000:02:00.0
               logical name: eth0
               version: 1b
               serial: XXXX
               size: 1Gbit/s
               capacity: 1Gbit/s
               width: 64 bits
               clock: 33MHz
               capabilities: pm msi pciexpress msix vpd bus_master cap_list ethernet physical
tp mii 10bt 10bt-fd 100bt 100bt-fd 1000bt-fd autonegotiation
```

```
                configuration: autonegotiation=on broadcast=yes driver=r8169
driverversion=6.3.13_1 duplex=full firmware=rtl8168h-2_0.0.2 02/26/15 ip=192.168.0.176
latency=0 link=yes multicast=yes port=twisted pair speed=1Gbit/s
                resources: irq:16 ioport:3000(size=256) memory:d1104000-d1104fff
memory:d1100000-d1103fff
```

```
Architecture:            x86_64
  CPU op-mode(s):        32-bit, 64-bit
  Address sizes:         39 bits physical, 48 bits virtual
  Byte Order:            Little Endian
CPU(s):                  8
  On-line CPU(s) list:   0-7
Vendor ID:               GenuineIntel
  BIOS Vendor ID:        Intel(R) Corporation
  Model name:            Intel(R) Core(TM) i3-10105T CPU @ 3.00GHz
    BIOS Model name:     Intel(R) Core(TM) i3-10105T CPU @ 3.00GHz  CPU @ 2.8GHz
    BIOS CPU family:     206
    CPU family:          6
    Model:               165
    Thread(s) per core:  2
    Core(s) per socket:  4
    Socket(s):           1
    Stepping:            3
    CPU(s) scaling MHz:  91%
    CPU max MHz:         3900.0000
    CPU min MHz:         800.0000
    BogoMIPS:            6000.00
    Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscp lm
constant_tsc art arch_perfmon pebs bts
                          rep_good nopl xtopology nonstop_tsc cpuid aperfmperf pni pclmulqdq
dtes64 monitor ds_cpl vmx est tm2 ssse3 sdbg fma cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic
movbe popcnt tsc_deadline_tim
                         er aes xsave avx f16c rdrand lahf_lm abm 3dnowprefetch cpuid_fault
epb invpcid_single ssbd ibrs ibpb stibp ibrs_enhanced tpr_shadow vnmi flexpriority ept vpid
ept_ad fsgsbase tsc_adjust b
                         mi1 avx2 smep bmi2 erms invpcid mpx rdseed adx smap clflushopt
intel_pt xsaveopt xsavec xgetbv1 xsaves dtherm ida arat pln pts hwp hwp_notify hwp_act_window
hwp_epp md_clear flush_l1d arc
                         h_capabilities
```

```
Virtualization features:
  Virtualization:        VT-x
Caches (sum of all):
  L1d:                   128 KiB (4 instances)
  L1i:                   128 KiB (4 instances)
  L2:                    1 MiB (4 instances)
  L3:                    6 MiB (1 instance)
NUMA:
  NUMA node(s):          1
  NUMA node0 CPU(s):     0-7
Vulnerabilities:
  Itlb multihit:         KVM: Mitigation: VMX disabled
  L1tf:                  Not affected
  Mds:                   Not affected
  Meltdown:              Not affected
  Mmio stale data:       Vulnerable: Clear CPU buffers attempted, no microcode; SMT vulnerable
  Retbleed:              Mitigation; Enhanced IBRS
  Spec store bypass:     Mitigation; Speculative Store Bypass disabled via prctl
  Spectre v1:            Mitigation; usercopy/swapgs barriers and __user pointer sanitization
  Spectre v2:            Mitigation; Enhanced / Automatic IBRS, IBPB conditional, RSB filling,
PBRSB-eIBRS SW sequence
  Srbds:                 Vulnerable: No microcode
  Tsx async abort:       Not affected
```

Revision #5
Created 2023-08-27 17:10:56 IST by hxd
Updated 2023-11-11 11:37:30 GMT by hxd