

Host Security ID: HSI:0! (v1.9.27)

HSI-1

- ✓ BIOS firmware updates: Enabled
- ✓ MEI key manifest: Valid
- ✓ csme override: Locked
- ✓ csme v0:16.50.0.1175: Valid
- ✓ Platform debugging: Disabled
- ✓ SPI write: Disabled
- ✓ Supported CPU: Valid
- ✓ TPM empty PCRs: Valid
- ✓ TPM v2.0: Found
- ✓ UEFI bootservice variables: Locked
- ✓ UEFI secure boot: Enabled
- ✗ csme manufacturing mode: Unlocked
- ✗ SPI lock: Disabled
- ✗ SPI BIOS region: Unlocked
- ✗ UEFI platform key: Invalid

HSI-2

- ✓ Intel BootGuard: Enabled
- ✓ IOMMU: Enabled
- ✓ Platform debugging: Locked
- ✓ TPM PCR0 reconstruction: Valid
- ✗ Intel BootGuard ACM protected: Invalid
- ✗ Intel BootGuard OTP fuse: Invalid
- ✗ Intel BootGuard verified boot: Invalid

HSI-3

- ✓ CET Platform: Supported
- ✓ Pre-boot DMA protection: Enabled
- ✗ Intel BootGuard error policy: Invalid
- ✗ Suspend-to-idle: Disabled
- ✗ Suspend-to-ram: Enabled

HSI-4

- ✓ SMAP: Enabled
- ✗ Encrypted RAM: Not supported

Runtime Suffix -!

- ✓ fwupd plugins: Untainted
- ✓ CET OS Support: Supported
- ✓ Linux kernel lockdown: Enabled
- ✓ Linux kernel: Untainted
- ✗ Linux swap: Unencrypted

This system has a low HSI security level.

» <https://fwupd.github.io/hsi.html#low-security-level>

This system has HSI runtime issues.

» <https://fwupd.github.io/hsi.html#hsi-runtime-suffix>

Host Security Events

2024-09-29 14:14:50:  CET OS Support changed: Not supported → Supported