hi,

I’m very confused about init-enclave sw hardening error.

Hyperthreading is switched to “Disabled” and no option available for overclocking/underclocking.

hw: Lenovo x1 extreme gen1, BIOS is patched (https://support.lenovo.com/sa/en/product_security/len-29846)

```
“ERROR [wasmi_runtime_enclave::registration::cert] Platform is updated but requires further BIOS configuration

ERROR [wasmi_runtime_enclave::registration::cert] The following vulnerabilities must be mitigated: [“INTEL-SA-00161”, “You must disable hyperthreading in the BIOS”, “INTEL-SA-00289”, “You must disable overclocking/undervolting in the BIOS”]

Platform status is SW_HARDENING_AND_CONFIGURATION_NEEDED. This means is updated but requires further BIOS configuration”
```

What’s happening? Wrong kernel, wrong sgx kernel module, wrong bios, wrong intel api calls or I just missed some BIOS option?

```
root@x1e:~# sgx-detect --verbose

Detecting SGX, this may take a minute…

SGX instruction set

CPU support

CPU configuration

Enclave attributes

Enclave Page Cache

SGX features

✘ SGX2 ✘ EXINFO ✘ ENCLV ✘ OVERSUB ✘ KSS

Total EPC size: 93.5MiB

✘ Flexible launch control

CPU support

CPU configuration

✘ Able to launch production mode enclave

SGX system software

SGX kernel device (/dev/isgx)

libsgx_enclave_common

AESM service

Able to launch enclaves

Debug mode

✘ Production mode

Production mode (Intel whitelisted)

  SGX system software > Able to launch enclaves > Production mode

The enclave could not be launched. This might indicate a problem with FLC.

debug: failed to load report enclave

debug: cause: failed to load report enclave

debug: cause: The EINITTOKEN provider didn’t provide a token
```

```
debug: cause: aesm error code GetLicensetokenError_6

More information: https://edp.fortanix.com/docs/installation/help/#run-enclave-prod

You’re all set to start running SGX programs!

root@x1e:~# uname -a

Linux x1e 5.4.0-48-generic #52~18.04.1-Ubuntu SMP Thu Sep 10 12:50:22 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

any ideas?