6.5. HWA-M4: System Not Appropriately Hardened

The embedded operating system was not suitably hardened to attack. This included having no security policies on the binaries and leaving unnecessary binaries and functionality on the system.

It is recommended that all unnecessary binaries are removed from the device and security properties are applied where possible.

Medium Risk
CVSS 4.4

Description

The device was found to be insufficiently hardened against attack. This was discovered in two key areas.

Firstly, [redacted]

[redacted]

Secondly, the key binaries in use, including the ones that have the ability to handle all input and output on the device, did not use the “NX” flag, stack canaries, or fortified function compiler flags. These all make it much harder to exploit issues such as buffer overflows.

```
┌──(kali㉿kali)-[~]
└─$ /opt/checksec.sh-2.6.0/./checksec --dir=./files/
RELRO           STACK CANARY      NX            PIE           RPATH      RUNPATH    Symbols         FORTIFY Fortified      Fortifiable   Filename
Partial RELRO   No canary found   NX enabled    No PIE        No RPATH   No RUNPATH   No Symbols       No    0              10              ./files/balena-engine
Partial RELRO   No canary found   NX enabled    No PIE        No RPATH   No RUNPATH   No Symbols       No    0              0               ./files/balena-engine-init
```

Figure 11: CheckSec running against binaries

[redacted]

Recommendations

[redacted]

Binaries should be compiled with appropriate compile-time hardening enabled.

Affected	[redacted]
References & CVSSv3 Metrics	Root Cause: Implementation Base Metrics: AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N (4.6) Temporal Metrics: E:H/RL:O/RC:C (4.4) Environmental Metrics: CR:M/IR:M/AR:M (4.4)