Hartwell Labs · business@hartwell-labs.pl · hartwell-labs.pl/firmware/

Sample extract · 24.11.2026

Firmware evidence pack — sample extract

This is a real extract from an audit of a **reference appliance image we build and audit ourselves** — not a client file. The numbers, hashes, paths and tool versions below were produced on 24.11.2026 and can be reproduced with the tools listed. Client reports are redacted the same way: the image hash identifies what was examined, never the customer.

1. What was examined

Item	Value
Image	bootable ISO, El Torito (BIOS + UEFI), 27 127 808 bytes
Kernel	6.12.118-0-lts (x86_64), 13 718 528 bytes
Initramfs	`boot/initrd`, 6 573 268 bytes compressed, 19 349 696 bytes unpacked
Root filesystem	gzip-compressed cpio archive, 16 apk packages
Application	one static binary, 1 302 856 bytes, not stripped
Secure boot material	`hartwell-db.cer` present in the ISO root

SHA-256 of the image examined:

`bee3b4ec54789736fef5b2606bcf50448d5ee96cfbac0a591daa5b2610be327b`

Members of the ISO, as listed by `bsdtar`:

```
boot/vmlinuz          13718528
boot/initrd            6573268
EFI/efiboot.img        6291456
isolinux/isolinux.bin    43008
hartwell-db.cer            804
```

2. SBOM

Produced with `syft 1.57.2` against the unpacked root filesystem, in both formats:

Format	Result
SPDX 2.3	67 packages
CycloneDX 1.6	198 components

The gap between the two numbers is the point of control 7. The 16 packages in the `apk` database are what the build system believes it installed. The other entries are kernel modules, an application binary and files the package manager never tracked. A supplier SBOM generated from the build recipe lists 16. The image contains 67.

OS packages found, with the exact versions scanned:

```
alpine-baselayout 3.7.0-r0      libapk2        2.14.9-r2
alpine-baselayout-data 3.7.0-r0 libcrypto3     3.5.0-r0
alpine-keys 2.5-r0              libssl3        3.5.0-r0
alpine-release 3.22.0-r0        musl           1.2.5-r10
apk-tools 2.14.9-r2             musl-utils     1.2.5-r10
busybox 1.37.0-r18              scanelf        1.3.8-r1
busybox-binsh 1.37.0-r18        ssl_client     1.37.0-r18
ca-certificates-bundle 20241121-r2 zlib        1.3.1-r2
```

3. Vulnerability match

Produced with `grype 0.122.1`, vulnerability database built 2026-11-24T06:22:05Z (schema v6.1.10), matching against the Alpine 3.22 advisory feed.

Severity	Findings	Unique CVEs
Critical	13	7
High	77	39
Medium	56	28
Low	18	8
Total	**164**	**82**

Twelve of the thirteen critical findings sit in one OpenSSL 3.5.0 build shipped twice under two package names, `libcrypto3 3.5.0-r0` and `libssl3 3.5.0-r0`. The thirteenth is `zlib 1.3.1-r2`. A fix exists for all of them upstream:

CVE	Package	Version found	Fixed in
CVE-2025-15467	libcrypto3, libssl3	3.5.0-r0	3.5.5-r0
CVE-2025-9230	libcrypto3, libssl3	3.5.0-r0	3.5.4-r0
CVE-2026-63073	libcrypto3, libssl3	3.5.0-r0	3.5.8-r0
CVE-2026-34182	libcrypto3, libssl3	3.5.0-r0	3.5.7-r0
CVE-2026-4738	zlib	1.3.1-r2	1.4-r0

4. One finding, with the evidence attached

Finding F-04 — cryptographic library out of date, reachable from the image's only network-facing code path.

- Image digest: `bee3b4ec54789736fef5b2606bcf50448d5ee96cfbac0a591daa5b2610be327b`
- File: `/usr/lib/libssl.so.3`, 839 544 bytes; `/usr/lib/libcrypto.so.3`, 4 973 328 bytes
- Package: `libssl3 3.5.0-r0`, `libcrypto3 3.5.0-r0` (`/lib/apk/db/installed`)
- Tool output: `grype 0.122.1`, 164 matches, 13 critical, all in this pair
- Consumer: `busybox ssl_client` is the only TLS client in the image; the fleet agent uses it for outbound HTTPS every 30 s

What that means in practice, and what it does not:

- the parsing code is present and is exercised by the agent on every poll, so the library is not dead weight;

- the device opens no listening socket — `netstat`-equivalent inspection of the rootfs shows no daemon, `root` password is locked (`root:*` in `/etc/shadow`), and there is no login service. A remote attacker cannot reach the library without something on the outbound path answering first;
- so severity depends on what the agent talks to. In this image that is a configured endpoint; a compromised or hostile server is the realistic path.

Verdict: **fix before shipping** — the upgrade is a package bump with no API change, and the cost of arguing reachability to an assessor is higher than the cost of rebuilding.

5. What we could not check, and why

Control	Status	What is needed
Update path, signature check	not tested in operation	a device or a test environment that can boot the image
Secure boot, chain of trust	material inspected, boot not exercised	OVMF/secboot run, or the device
Runtime behaviour of the agent	not tested	endpoint, credentials, and a capture
Anything physical	out of scope	teardown, chip-off and SPI dump are not our work

6. What a partner receives

This extract in full, plus: the SPDX and CycloneDX files, the raw `grype` JSON, the hash manifest for the image and every unpacked partition, and a one-page summary written for the person who signs the file. Delivered under the partner's template and name; our name appears in the NDA and nowhere else.