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, the device was running a default instance of BusyBox which included all functions, a large amount of which were not required for maintenance of the device. It is common to remove any functions that are not required to provide a smaller attack surface on the device.

```
root@[redacted]:~# busybox
BusyBox v1.31.1 () multi-call binary.
BusyBox is copyrighted by many authors between 1998-2015.
Licensed under GPLv2. See source distribution for detailed
copyright notices.

Usage: busybox [function [arguments]...]
   or: busybox --list
   or: busybox --show SCRIPT
   or: function [arguments]...

        BusyBox is a multi-call binary that combines many common Unix
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use and BusyBox
        will act like whatever it was invoked as.

Currently defined functions:
        [, [[, addgroup, adduser, arch, ash, awk, basename, bc, blkdiscard, blkid,
bunzip2, bzcat, cat, chattr, chgrp, chmod, chown, chroot, chvt, clear, cmp, cp,
cpio, cut, date, dc, dd, deallocvt, delgroup, deluser, depmod, df, diff, dirname,
dmesg, dnsdomainname, du,
        dumpkmap, dumpleases, echo, egrep, env, expr, factor, fallocate, false,
fbset, fdisk, fgrep, find, flock, free, fsck, fsfreeze, fstrim, fuser, getopt,
getty, grep, groups, gunzip, gzip, halt, head, hexdump, hexedit, hostname, hwclock,
i2ctransfer, id, ifconfig, ifdown,
        ifup, insmod, ip, ipneigh, kill, killall, klogd, link, linux32, linux64,
linuxrc, ln, loadfont, loadkmap, logger, logname, logread, losetup, ls, lsmod,
lsscsi, lzcat, md5sum, mesg, microcom, mkdir, mkdosfs, mke2fs, mkfifo, mknod,
mkpasswd, mkswap, mktemp, modprobe, more,
        mount, mv, nc, netstat, nl, nohup, nologin, nproc, nsenter, nslookup, nuke,
od, openvt, partprobe, paste, patch, pidof, pivot_root, poweroff, printf, ps, pwd,
rdate, readlink, realpath, reboot, renice, reset, resize, resume, rfkill, rm,
rmdir, rmmod, route, run-init,
        run-parts, sed, seq, setconsole, setfattr, setpriv, sh, sha1sum, sha256sum,
shred, shuf, sleep, sort, ssl_client, start-stop-daemon, stat, strings, stty,
sulogin, svc, svok, swapoff, swapon, switch_root, sync, sysctl, syslogd, tail, tar,
tc, tee, telnet, test, tftp,
        time, top, touch, tr, true, ts, tty, ubirename, udhcpc, udhcpd, umount,
uname, uniq, unlink, unshare, unzip, uptime, users, usleep, vi, w, watch, wc, wget,
which, who, whoami, xargs, xxd, xzcat, yes, zcat
root@bcef0a1:~#
```