Hard-coded Default Root Credentials for All ecobee3 lite Devices

UNRANKED

ADVISORY ID	L9-15-160
PUBLISHED	June 28, 2021
UPDATED	August 19, 2021
CATEGORY	Global Default Credentials
VENDOR	ecobee
PRODUCT	ecobee3 lite
VERSION	4.5.81.200

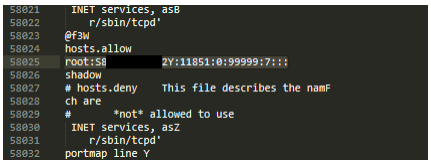
Risk Summary

Hard-coded default root credentials exist across all devices, potentially allowing a threat actor to gain privileged access to the ecobee3 lite device. The root passwords reserved for admin users can be discovered through analysis of the compiled firmware via reverse engineering. The password is stored in a hash format but lacks complexity and can be easily brute-forced. Using the cracked password a threat actor can gain access to the serial console on the device. The threat actor could use this privilege to extract sensitive information or modify the device.

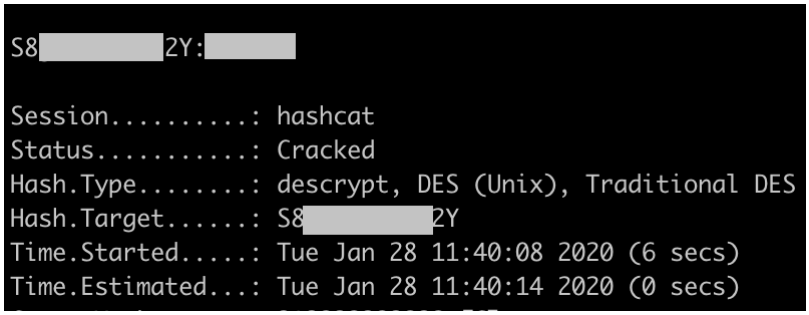
Technical Details

The research team extracted the root credentials by extracting the contents of the NAND flash. The credentials were cracked using brute force techniques. The credentials were used to gain access to the password protected serial console.

Credential firmware dump



Cracked passwords



Root access

```
/config # id
uid=0(root) gid=0(root)
/config # ls -la
drwxr-xr-x   14 root     root         3408 Jun 12  2020 .
drwxrwxr-x   18 514      514          1328 Feb  7  2020 ..
-rw-r--r--    1 root     root         6916 Jun 12  2020 alert_reminders.xml
lrwxrwxrwx    1 root     root           26 Feb  6  2020 backplate.hex -> /idt/backplate-2.0.208.hex
drwxr-xr-x    2 root     root          160 Jan  1  1970 bootImage
-rw-r--r--    1 root     root          153 Feb  7  2020 compressorMinOutTemp.json
-rw-r--r--    1 root     root          153 Feb  7  2020 compressorMinOutTemp2.json
drwxr-xr-x    2 root     root          160 Jan  1  1970 contractorImage
-rw-r--r--    1 root     root            0 Jun 12  2020 curl_debug.log
drwxrwxrwx    2 root     root          160 Apr 16  2019 default
-rw-r--r--    1 root     root          228 Feb  6  2020 dev_manager.json
-rw-r--r--    1 root     root          228 Feb  6  2020 dev_manager2.json
drwxr-xr-x    2 root     root          232 Feb  7  2020 developer
-rwx------    1 root     root            0 May  7  2014 dntrylegacysslport.tag
drwxr-xr-x    2 root     root          160 Jan  1  1970 eiImage
-rw-r--r--    1 root     root            0 Jun 12  2020 experimentRunnerWatchdogLog
-rw-r--r--    1 root     root          299 Feb  8  2020 feelslike.json
-rw-r--r--    1 root     root          299 Feb  8  2020 feelslike2.json
-rw-r--r--    1 root     root           38 Jan 28  2020 firstTimeOnly.log
drwxrwxrwx    2 root     root          160 Apr 16  2019 golden
-rw-r--r--    1 root     root          147 Feb  6  2020 homekit.json
-rw-r--r--    1 root     root          147 Feb  6  2020 homekit2.json
-rw-r--r--    1 root     root          122 Jun 12  2020 hvacTempData.xml
drwxr-xr-x    2 root     root          160 Feb  7  2020 idtImage
lrwxrwxrwx    1 root     root           19 Feb  6  2020 idtm -> /idt/idtm-4.5.57.76
lrwxrwxrwx    1 root     root           24 Feb  6  2020 images.mmz -> /idt/images-4.5.57.1.mmz
drwxr-xr-x    2 root     root          624 Jan 28  2020 keys
-rw-r--r--    1 root     root          240 Feb  8  2020 lastOnTimes
lrwxrwxrwx    1 root     root           25 Feb  6  2020 libcore.so -> /idt/libcore-4.5.57.41.so
lrwxrwxrwx    1 root     root           26 Feb  6  2020 libfonts.so -> /idt/libfonts-4.5.57.36.so
lrwxrwxrwx    1 root     root           28 Feb  6  2020 libhomekit.so -> /idt/libhomekit-4.5.57.41.so
lrwxrwxrwx    1 root     root           30 Feb  6  2020 libwacserver.so -> /idt/libwacserver-4.5.57.41.so
lrwxrwxrwx    1 root     root           25 Feb  8  2020 libwifi.so -> /idt/libwifi-4.5.57.41.so
lrwxrwxrwx    1 root     root           25 Feb  6  2020 libwifi.so.bak -> /idt/libwifi-4.5.57.41.so
-rw-r--r--    1 root     root           72 Feb  8  2020 outdoorMinTempDB.xml
drwxr-xr-x    2 root     root          248 Feb  7  2020 patch
-rw-r--r--    1 root     root           32 Feb  6  2020 secretkey.key
-rw-r--r--    1 root     root          131 Jun 12  2020 stacktrace
-rw-r--r--    1 root     root        29369 Jun 12  2020 stacktrace_history
-rw-r--r--    1 root     root        27005 Feb  7  2020 thermostat3.xml
-rw-r--r--    1 root     root        27005 Feb  8  2020 thermostat3.xml.sync
drwxr-xr-x    2 root     root          488 Feb  7  2020 tools
drwxr-xr-x    2 root     root          160 Jan  1  1970 userImage
drwxr-xr-x    2 root     root          160 Jan  1  1970 utilityImage
-rw-r--r--    1 root     root          881 Feb  7  2020 wifi_config.json
-rw-r--r--    1 root     root          881 Feb  7  2020 wifi_config2.json
/config #
```

Debug port password

```
U-Boot 2009.08-svn136919 (Jun 17 2016 - 15:02:18) (Nike)

Freescale i.MX28 family
CPU:   454 MHz
BUS:   151 MHz
EMI:   166 MHz
GPMI:   24 MHz
DRAM:  128 MB
NAND:  Manufacturer      : AMD (0x01)
Device Code       : 0xf1
Cell Technology   : SLC
Chip Size         : 128 MiB
Pages per Block   : 64
Page Geometry     : 2048+64
ECC Strength      : 1 bits
ECC Size          : 512 B
Data Setup Time   : 20 ns
Data Hold Time    : 10 ns
Address Setup Time: 20 ns
GPMI Sample Delay : 6 ns
tREA              : Unknown
tRLOH             : Unknown
tRHOH             : Unknown
Description       : S34ML01G1
128 MiB
Using default environment

LCD IC Identification is 0x00779600 !
Doing Startek Init....
In:    serial
Out:   serial
Err:   serial
Net:   No ethernet found.
uboot version: 1.4.2 (0x10402)
Initial Boot Mode = 3
Received 8 B message F2 with bad CRC: calc = 0x20F3 received = 0xD714
Received RTC time = 1591990036
Get DATE: 2020-06-12 (wday=5)  TIME: 19:27:16
RTC Time = 06-12-2020 19:27:16
top guard: b001c041
00: 5ee3cc78
01: 5ee3d714
02: 0
03: 0
04: 0
05: 0
06: 0
07: 0
08: 0
09: 0
bot guard: b001c041
Final Boot Mode = 3
uboot flash version=0x10402  usegolden=0x0
Updating bootinfo
Note: Using default kernel and root.
bootcmd="run bootargs_default; watchdog; nand read ${loadaddr} 1F00000 400000; bootm ${loadaddr}"
Enter the password to stop autoboot:  0
```