# Remote Denial of Service of ecobee3 lite

UNRANKED

| | |
|---|---|
| ADVISORY ID | L9-15-163 |
| PUBLISHED | June 28, 2021 |
| UPDATED | August 19, 2021 |
| CATEGORY | Null Dereference |
| VENDOR | ecobee |
| PRODUCT | ecobee3 lite |
| VERSION | 4.5.81.200 |

## Risk Summary

A threat actor sharing the same network as the Ecobee3 can craft a malicious HTTP request which will cause the device to crash and reboot.

## Technical Details

The Wireless Access Configuration (WAC) server used to connect the ecobee3 device to the WiFi networking using an Apple device crashes when a specially crafted web request is received.

### POST request


A threat actor can send a POST request to the endpoint http://<thermostat_ip>:1200/config and omit the 'Content-Type' header which causes the 'HKProcessConfig==>memcpy' function to read from the address space 0x00000000 causing the main application (idtm) to crash. Once a crash has occurred the 'watchdog' will cause the device to reset.

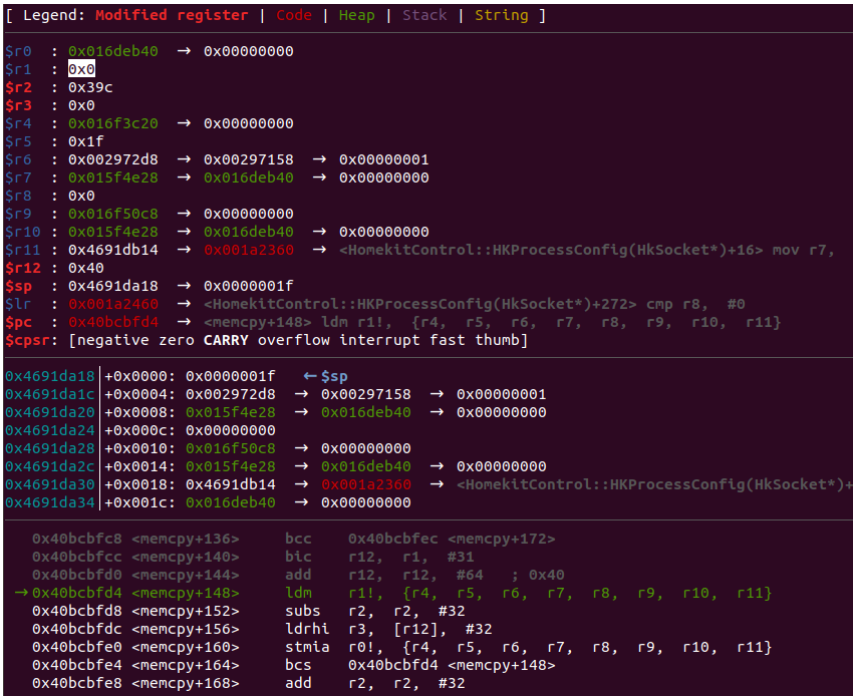
### Normal operations

```
[ Legend: Modified register | Code | Heap | Stack | String ]
$r0  : 0x016dd3a0  →  0x00000000
$r1  : 0x0187fb00  →  0x41414141  →  0x00000000
$r2  : 0x4f3
$r3  : 0x18
$r4  : 0x41414141  →  0x00000000
$r5  : 0x41414141  →  0x00000000
$r6  : 0x41414141  →  0x00000000
$r7  : 0x41414141  →  0x00000000
$r8  : 0x41414141  →  0x00000000
$r9  : 0x41414141  →  0x00000000
$r10 : 0x016f4730  →  0x016dd388  →  0x41414141  →  0x00000000
$r11 : 0x4691db14  →  0x001a2360  →  <HomekitControl::HKProcessConfig(HkSocket*)+16> mov r7,  r0
$r12 : 0x0187fb40  →  0x41414141  →  0x00000000
$sp  : 0x4691da18  →  0x0000001e
$lr  : 0x001a2460  →  <HomekitControl::HKProcessConfig(HkSocket*)+272> cmp r8,  #0
$pc  : 0x40bcbfd4  →  <memcpy+148> ldm r1!,  {r4,  r5,  r6,  r7,  r8,  r9,  r10,  r11}
$cpsr: [negative zero CARRY overflow interrupt fast thumb]

0x4691da18 |+0x0000: 0x0000001e   ←$sp
0x4691da1c |+0x0004: 0x002972d8  →  0x00297158  →  0x00000001
0x4691da20 |+0x0008: 0x016f4730  →  0x016dd388  →  0x41414141  →  0x00000000
0x4691da24 |+0x000c: 0x00000000
0x4691da28 |+0x0010: 0x016df688  →  0x00000000
0x4691da2c |+0x0014: 0x016f4730  →  0x016dd388  →  0x41414141  →  0x00000000
0x4691da30 |+0x0018: 0x4691db14  →  0x001a2360  →  <HomekitControl::HKProcessConfig(HkSocket*)+16> mov r7,  r0
0x4691da34 |+0x001c: 0x016dd388  →  0x41414141  →  0x00000000

   0x40bcbfc8 <memcpy+136>     bcc    0x40bcbfec <memcpy+172>
   0x40bcbfcc <memcpy+140>     bic    r12,  r1,  #31
   0x40bcbfd0 <memcpy+144>     add    r12,  r12,  #64   ; 0x40
 →0x40bcbfd4 <memcpy+148>     ldm    r1!,  {r4,  r5,  r6,  r7,  r8,  r9,  r10,  r11}
   0x40bcbfd8 <memcpy+152>     subs   r2,  r2,  #32
   0x40bcbfdc <memcpy+156>     ldrhi  r3,  [r12],  #32
   0x40bcbfe0 <memcpy+160>     stmia  r0!,  {r4,  r5,  r6,  r7,  r8,  r9,  r10,  r11}
   0x40bcbfe4 <memcpy+164>     bcs    0x40bcbfd4 <memcpy+148>
   0x40bcbfe8 <memcpy+168>     add    r2,  r2,  #32
```

Crash dump




Device crash

```
[Info]HomeKit QR Code URI: X-HM:
[Info]Connecting 32 numConnections=1
[Info]Handling /config
signal caught: 11
IfaceThreadLine=8 InterfaceThreadLineNum=-1 InterfaceDeleteAllRoutesLine=-1 IfaceUpDownThreadLine=-1  LightControlLine=0
InterfaceSetAddrLine=112 WifiScanThreadLine=-1 WifiScanListLine=-1 WifiConfigDeviceLine=7 HKControlThreadLine=3 WatchdogLine=2
ExperimentRunnerThreadMainLoop=1 ExperimentRunnerThreadRefresh=1 ExperimentRunnerThreadBinaryDownload=1 ExperimentRunnerThreadWatchdog=1 ExperimentRunnerThreadCurl=-1
Animation=10001 -10 CurrentScreen=10001 CreateScreenSaver
Process Crashed!!  ThreadID=1177547872  Threadname=Unknown
>> 4          :   build:4.5.81.200   crash at 2020-06-24 17:02:23
idtbacktrace dump of 6 Return Addresses
0x462fe660:   0x00070ac4 (0x000703dc = signalHandler(int) + 0x000006e8)
0x462fe718:   0x40b75e50 (0x4060ffec = _fini + 0x00565e64)
0x462feb08:   0x001ac664 (0x001aa038 = HomekitControl::threadProcess(void*) + 0x0000262c)
0x462feda0:   0x001ada78 (0x001ada64 = HomekitControl::runThread(void*) + 0x00000014)
0x462fedb0:   0x401e8224 (0x401e8204 = ecobee::Threading::IDTThread::threadEntry(void*) + 0x00000020)
0x462fedc8:   0x40b2c038 (0x4060ffec = _fini + 0x0051c04c)
libc dump of 9 Return Addresses
0x00070840 (0x000703dc = signalHandler(int) + 0x00000464)
0x40b75e50 (0x4060ffec = _fini + 0x00565e64)
0x40bcbfa8 (0x4060ffec = _fini + 0x005bbfbc)
0x001a2460 (0x001a2350 = HomekitControl::HKProcessConfig(HkSocke*) + 0x00000110)
0x001ac664 (0x001aa038 = HomekitControl::threadProcess(void*) + 0x0000262c)
0x001ada78 (0x001ada64 = HomekitControl::runThread(void*) + 0x00000014)
0x401e8224 (0x401e8204 = ecobee::Threading::IDTThread::threadEntry(void*) + 0x00000020)
0x40b2c038 (0x4060ffec = _fini + 0x0051c04c)
0x40c207a8 (0x4060ffec = _fini + 0x006107bc)
libc dump of 9 backtrace symbols
/config/idtm(_Z13signalHandleri+0x464) [0x70840]
/lib/libc.so.6(__default_sa_restorer_v2+0) [0x40b75e50]
/lib/libc.so.6(memcpy+0x68) [0x40bcbfa8]
/config/idtm(_ZN14HomekitControl15HKProcessConfigEP8HkSocket+0x110) [0x1a2460]
/config/idtm(_ZN14HomekitControl13threadProcessEPv+0x262c) [0x1ac664]
/config/idtm(_ZN14HomekitControl9runThreadEPv+0x14) [0x1ada78]
libcore.so(_ZN6ecobee9Threading9IDTThread11threadEntryEPv+0x20) [0x401e8224]
/lib/libpthread.so.0(+0x7038) [0x40b2c038]
/lib/libc.so.6(clone+0x88) [0x40c207a8]
top_frame: 0x0x462fe660, top_stack: 0x0x462fe63f  stack_end: 0x0x462feff0
WatchdogLine=2
Animation=10001 -10  CurrentScreen=10001 CreateScreenSaver
Animation=10001 -10  CurrentScreen=10001 CreateScreenSaver
dump crashdebug
00: 24-16:49:08 newscreen 10001 CreateScreenSaver
<< Process Crashed!!  ProcessID=562  Threadname=Unknown
Wrote LastOnInfo to NAND
```