Talos Vulnerability Report

TALOS-2021-1230

Trend Micro, Inc. Home Network Security tdts.ko chrdev_ioctl_handle privilege escalation vulnerability

MAY 24, 2021

CVE NUMBER

CVE-2021-32457

Summary

A privilege escalation vulnerability exists in the tdts.ko chrdev_ioctl_handle functionality of Trend Micro, Inc. Home Network Security 6.1.567. A specially crafted ioctl can lead to increased privileges. An attacker can issue an ioctl to trigger this vulnerability.

Tested Versions

Trend Micro, Inc. Home Network Security 6.1.567

Product URLs

https://www.trendmicro.com/en_us/forHome/products/homenetworksecurity.html

CVSSv3 Score

7.8 - CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-121 - Stack-based Buffer Overflow

Details

The Home Network Security Station is a device used to monitor and protect home networks from security threats as well as offer simple network management features. The Station provides vulnerability scanning, web threat protection, intrusion prevention, as well as device-based access control for all devices on a home network.

This vulnerability is caused by the lack of input validation on a user's `ioctl` request from user land. The upper 16 bits from the ioctl request (AND with 0x3FFF, so 14 bits total) are blindly used as input to `__memzero` to a stack-based buffer in kernel space. The stack-based buffer is smaller than the maximum ioctl request copy size of 0x3FFF and thus overflows. A user can leverage this to write \x00 to a large portion of the kernel stack causing a kernel panic and in turn, a denial of service. This could potentially also be leveraged into a privilege escalation vulnerability.

```
chrdev_ioctl_handle:
0000074c  10402de9   push    {r4, lr} {__saved_lr} {__saved_r4}
00000750  5034e7e7   ubfx    r3, r0, #0x8, #0x8
00000754  be0053e3   cmp     r3, #0xbe
00000758  1800e013   mvnne   r0, #0x18  {0xffffffe7}
0000075c  38d04de2   sub     sp, sp, #0x38
00000760  2900001a   bne     0x80c

// Check that the bits 8-15 are 0xbe in the IOCTL request
00000764  ff0010e3   tst     r0, #0xff
00000768  1500e003   mvneq   r0, #0x15  {0xffffffea}
0000076c  2600000a   beq     0x80c

00000770  0d20a0e1   mov     r2, sp {var_40}
00000774  000050e3   cmp     r0, #0
00000778  7f3dc2e3   bic     r3, r2, #0x1fc0 {var_40}
// Extract the size of the buffer encoded in the IOCTL request
0000077c  5028ede7   ubfx    r2, r0, #0x10, #0xe
00000780  3f30c3e3   bic     r3, r3, #0x3f
00000784  380000ba   blt     0x86c

// Sanity checks to make sure that the encoded size is not negative
0000086c  084093e5   ldr     r4, [r3,  #0x8]
00000870  020091e0   add.s   r0, r1, r2
00000874  0400d030   sbc.slo r0, r0, r4
00000878  0040a033   movlo   r4, #0
0000087c  000054e3   cmp     r4, #0
00000880  c3ffff0a   beq     0x794

00000794  083093e5   ldr     r3, [r3,  #0x8]
00000798  020091e0   add.s   r0, r1, r2
0000079c  0300d030   sbc.slo r0, r0, r3
000007a0  0030a033   movlo   r3, #0
000007a4  000053e3   cmp     r3, #0
000007a8  2a00000a   beq     0x858

// Ensure that r2 is not zero
000007ac  000052e3   cmp     r2, #0
000007b0  3400001a   bne     0x888

// Vulnerable __memzero with user provided length and set size stack-buffer
00000888  0d00a0e1   mov     r0, sp {var_40}
0000088c  0210a0e1   mov     r1, r2
00000890  b16901eb   bl      __memzero
```

Crash Information

```
Unable to handle kernel NULL pointer dereference at virtual address 00000000
pgd = 8faac000
[00000000] pgd=6b222831, pte=00000000, ppte=00000000
Internal error: Oops: 80000017 [#1] SMP ARM
Modules linked in: kmdiamond(O) tdtsudb(PO) tdts(PO)
CPU: 0 PID: 1539 Comm: poc2 Tainted: P           O 3.10.70 #2
task: 8f966000 ti: 8fad2000 task.ti: 8fad2000
PC is at 0x0
LR is at 0x0
pc : [<00000000>]    lr : [<00000000>]    psr: 00000013
sp : 8fad3f28  ip : 00000000  fp : 7efffc24
r10: 00000000  r9 : 8fad2000  r8 : 8fae9540
r7 : 00000003  r6 : 8fae9540  r5 : ffffffff  r4 : 00000000
r3 : 00000000  r2 : 00000000  r1 : ffffffff  r0 : fffffff2
Flags: nzcv  IRQs on  FIQs on  Mode SVC32  ISA ARM  Segment user
Control: 10c53c7d  Table: 6faac06a  DAC: 00000015
Process poc2 (pid: 1539, stack limit = 0x8fad2238)
Stack: (0x8fad3f28 to 0x8fad4000)
3f20:                   00000000 00000000 00000000 00000000 00000000 00000000
3f40: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
3f60: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
3f80: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
3fa0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
3fc0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
3fe0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
Code: bad PC value
---[ end trace 7b9adcd427e025e9 ]---
Dec  2 21:12:17 Diamond user.alert kernel: Unable to handle kernel NULL pointer dereference at virtual address 00000000
Dec  2 21:12:17 Diamond user.alert kernel: pgd = 8faac000
Dec  2 21:12:17 Diamond user.alert kernel: [00000000] pgd=6b222831, pte=00000000, ppte=00000000
Dec  2 21:12:17 Diamond user.emerg kernel: Internal error: Oops: 80000017 [#1] SMP ARM
Dec  2 21:12:17 Diamond user.warn kernel: Modules linked in: kmdiamond(O) tdtsudb(PO) tdts(PO)
Dec  2 21:12:17 Diamond user.warn kernel: CPU: 0 PID: 1539 Comm: poc2 Tainted: P           O 3.10.70 #2
Dec  2 21:12:17 Diamond user.warn kernel: task: 8f966000 ti: 8fad2000 task.ti: 8fad2000
Dec  2 21:12:17 Diamond user.warn kernel: PC is at 0x0
Dec  2 21:12:17 Diamond user.warn kernel: LR is at 0x0
Dec  2 21:12:17 Diamond user.warn kernel: pc : [<00000000>]    lr : [<00000000>]    psr: 00000013Unable to handle kernel NULL pointer
dereference at virtual address 00000000
pgd = 8fa68000
[00000000] pgd=6f924831, pte=00000000, ppte=00000000
Internal error: Oops: 80000017 [#2] SMP ARM
Modules linked in: kmdiamond(O) tdtsudb(PO) tdts(PO)
CPU: 0 PID: 559 Comm: syslogd Tainted: P      D    O 3.10.70 #2
task: 8f92c3c0 ti: 8fa60000 task.ti: 8fa60000
PC is at 0x0
LR is at calltimerfn.isra.35+0x24/0x84
pc : [<00000000>]    lr : [<8002cabc>]    psr: 60000113
sp : 8fa61d90  ip : 00000000  fp : 00000004
r10: 00000001  r9 : 80548894  r8 : 805140c0
r7 : 00000000  r6 : 00000100  r5 : 8fa60000  r4 : 8fa60010
r3 : 8fa61d90  r2 : 00000000  r1 : 00000000  r0 : 00000000
Flags: nZCv  IRQs on  FIQs on  Mode SVC32  ISA ARM  Segment user
Control: 10c53c7d  Table: 6fa6806a  DAC: 00000015
Process syslogd (pid: 559, stack limit = 0x8fa60238)
Stack: (0x8fa61d90 to 0x8fa62000)
1d80:                                     00000000 00000022 8f8059c0 80548080
1da0: 8fa61db0 00000000 00200200 8002cc9c 8fa61db0 8fa61db0 ffffbfcc 00000101
1dc0: 80514084 00000004 8fa60000 00000100 8fa60018 80026d2c 00000001 00015220
1de0: 00000000 805106c0 80547e40 0000000a ffffbfcd 805140c0 80526524 00400040
1e00: 00000000 60000193 00000022 00000000 f8200100 8f1d7e00 8f86f410 a0000013
1e20: 8f87e061 80026ea4 80510cc4 800270e0 80510cc4 8000ee44 f820010c 8051a7f8
1e40: 8fa61e60 8000857c 803aaf18 60000013 ffffffff 8fa61e94 8f1d7e00 8000db80
1e60: 8f86f410 60000013 00000070 00006adc 00000000 8f819000 00000000 00000061
1e80: 8f1d7e00 8f86f410 a0000013 8f87e061 00000000 8fa61ea8 801daac8 803aaf18
1ea0: 60000013 ffffffff 801daa18 00000062 8f87e000 8f1d7e00 8fa00a70 8fa60010
1ec0: 8fa00800 803c1ab8 8fae99c0 801c4b2c 00000000 8f87e000 00000000 8f1d7f4c
1ee0: 8ad51000 00000000 8f92c3c0 800480dc 8f1d7f50 8f1d7f50 00000041 00000062
1f00: 8f1d7e00 000be334 00000062 8fae99c0 00000000 8fa60000 8fa60000 801c1a04
1f20: 8f442080 801c4860 8f1d2380 00000062 00000000 8fae99c0 00000062 000be334
1f40: 8fa61f80 801c1bac 00000062 00000000 7ef0ac14 800bf350 8ad51000 8fae99c8
1f60: 8f442080 8fae99c0 000be334 00000000 00000000 00000000 00000062 800bf8c4
1f80: 00000000 00000000 00000000 000bde08 00000062 000be334 00000004 8000e0e8
1fa0: 8fa60000 8000df40 000bde08 00000062 00000005 000be334 00000062 00000000
1fc0: 000bde08 00000062 000be334 00000004 00000001 000bde40 00000062 7ef0ac14
1fe0: 00000000 7ef0ab54 0001d488 76f0100c 60000010 00000005 00000000 00000000
[<8002cabc>] (calltimerfn.isra.35+0x24/0x84) from [<8002cc9c>] (runtimersoftirq+0x180/0x204)
[<8002cc9c>] (runtimersoftirq+0x180/0x204) from [<80026d2c>] (dosoftirq+0x108/0x1e0)
[<80026d2c>] (dosoftirq+0x108/0x1e0) from [<80026ea4>] (dosoftirq+0x50/0x58)
[<80026ea4>] (dosoftirq+0x50/0x58) from [<800270e0>] (irqexit+0x5c/0x94)
[<800270e0>] (irqexit+0x5c/0x94) from [<8000ee44>] (handleIRQ+0x44/0x90)
[<8000ee44>] (handleIRQ+0x44/0x90) from [<8000857c>] (gichandleirq+0x2c/0x5c)
[<8000857c>] (gichandleirq+0x2c/0x5c) from [<8000db80>] (irqsvc+0x40/0x50)
Exception stack(0x8fa61e60 to 0x8fa61ea8)
1e60: 8f86f410 60000013 00000070 00006adc 00000000 8f819000 00000000 00000061
1e80: 8f1d7e00 8f86f410 a0000013 8f87e061 00000000 8fa61ea8 801daac8 803aaf18
1ea0: 60000013 ffffffff
[<8000db80>] (irqsvc+0x40/0x50) from [<803aaf18>] (rawspinunlockirqrestore+0x1c/0x20)
[<803aaf18>] (rawspinunlockirqrestore+0x1c/0x20) from [<801daac8>] (uartwrite+0xb0/0xd0)
[<801daac8>] (uartwrite+0xb0/0xd0) from [<801c4b2c>] (nttywrite+0x2cc/0x450)
[<801c4b2c>] (nttywrite+0x2cc/0x450) from [<801c1a04>] (ttywrite+0x10c/0x2b4)
[<801c1a04>] (ttywrite+0x10c/0x2b4) from [<800bf350>] (vfswrite+0xb0/0x194)
[<800bf350>] (vfswrite+0xb0/0x194) from [<800bf8c4>] (SySwrite+0x3c/0x78)
[<800bf8c4>] (SySwrite+0x3c/0x78) from [<8000df40>] (retfastsyscall+0x0/0x30)
Code: bad PC value
---[ end trace 7b9adcd427e025ea ]---
Kernel panic - not syncing: Fatal exception in interrupt***
```

Timeline

2021-01-22 - Vendor Disclosure

2021-04-06 - 75+ day follow up

2021-04-20 - Talos granted timeline extension for disclosure

2021-05-20 - Vendor Patched

2021-05-24 - Public Release

CREDIT

Discovered by Carl Hurd and Kelly Leuschner of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2020-1142

NEXT REPORT

TALOS-2021-1231