Talos Vulnerability Report

TALOS-2022-1476

# InHand Networks InRouter302 console factory stack-based buffer overflow vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-26002

## Summary

A stack-based buffer overflow vulnerability exists in the console factory functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted network request can lead to remote code execution. An attacker can send a sequence of malicious packets to trigger this vulnerability.

## Tested Versions

InHand Networks InRouter302 V3.5.4

## Product URLs

InRouter302 - https://www.inhandnetworks.com/products/inrouter300.html

## CVSSv3 Score

9.1 - CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H 9.9 - CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H - chain: TALOS-2022-1472
### CWE

CWE-121 - Stack-based Buffer Overflow

## Details

The InRouter302 is an industrial LTE router. It features remote management functionalities and several security protection mechanism, such as: VPN technologies, firewall functionalities, authorization management and several other features.

The InRouter302 offers the telnet and sshd services. Both, when provided with the correct credentials, will allow access to the Router console.

Here is the prompt after the login:

```
**********************************************
        Welcome to Router console
    Inhand
    Copyright @2001-2020, Beijing InHand Networks Co., Ltd.
    http://www.inhandnetworks.com
----------------------------------------------
Model                : IR302-WLAN
Serial Number        : RF3022141057211
Description          : www.inhandnetworks.com
Current Version      : V3.5.4
Current Bootloader Version : 1.1.3.r4955
----------------------------------------------
get help for commands
----------------------------------------------
type '?' for detail help at any point
==============================================
help           -- get help for commands
language       -- Set language
show           -- show system information
exit           -- exit current mode/console
ping           -- ping test
comredirect    -- COM redirector
telnet         -- telnet to a host
traceroute     -- trace route to a host
enable         -- turn on privileged commands
Router>
```

Several commands are available. The Router console offers, given the privileged user password, additional privileged functionalities. Here is the prompt after providing the privileged user credentials:

```
Router> enable
input password:
Router#
get help for commands
-----------------------------------------------
type '?' for detail help at any point
===============================================
help           -- get help for commands
language       -- Set language
show           -- show system information
exit           -- exit current mode/console
reboot         -- reboot system
ping           -- ping test
comredirect    -- COM redirector
telnet         -- telnet to a host
traceroute     -- trace route to a host
disable        -- turn off privileged commands
configure      -- enter configuration mode
restore        -- restore firmware
erase          -- erase a filesystem
Router#
```

The Router console contains a command, called `factory`, that is not listed among the available functionalities. This is probably a leftover debug code.

Here is the function that will manage the `factory` command in the privileged user level:

```
int factory_functionality(undefined4 param_1,char *command_line_provided)

{
  [...]

  if ((command_line_provided == (char *)0x0) || (*command_line_provided == '\0')) {
    is_command = -2;
  }
  else {
    second_arg = command_line_provided;
    first_arg = (char *)maybe_get_next_token(second_arg);
    [...]
    is_command = strncmp(first_arg,"iwpriv",6);
[1]
    if (is_command != 0) {
      return 0;
    }
    if (*second_arg == '\"') {
      second_arg = second_arg + 1;
    }
    second_arg_ = second_arg;
    [...]
    sprintf(command_line_buff,"iwpriv %s",second_arg_);
[2]
    system(command_line_buff);
[3]
  }
  [...]
}
```

The `command_line_provided` argument is what follows the `factory` command. The command is split, using the space, into two tokens. If the first token provided is `iwpriv`, checked at `[1]`, then later the second token, at `[2]`, will be used to create the `iwpriv <second_token>` command. This command will be executed, at `[3]`, with `system`.

The `sprintf`, executed at `[2]`, is performed using the second command line token. The provided token is ensured to be, at most, 128 bytes, which is exactly the length of the buffer. Because the second token is inserted after the string `iwpriv ` , the `sprintf` can lead to a stack-based buffer overflow in the `command_line_buff` buffer.

The epilogue of the `factory_functionality` function is the following:

```
00403eb0 a4 00 bf 8f     lw                              ra, 0xa4(sp)=>local_4
00403eb4 21 10 00 02     move                            v0, s0
00403eb8 a0 00 b2 8f     lw                              s2, 0xa0(sp)=>local_8
00403ebc 9c 00 b1 8f     lw                              s1, 0x9c(sp)=>local_c
[4]
00403ec0 98 00 b0 8f     lw                              s0, 0x98(sp)=>local_10
[5]
00403ec4 08 00 e0 03     jr                              ra
```

Because the `command_line_buff` is at offset `$sp+0x18`, it is possible to overwrite entirely `$sp+0x98` and 3 bytes from `$sp+0x9c`. So, because at `[4]` and `[5]` those value are moved inside `$s0` and `$s1` respectively, those registers are controllable. In particular the control of `$s0` can lead to code execution.

Note that, while this issue requires the most privileged logged-in user, it's possible to use TALOS-2022-1472 to perform this API starting from low-privileged user credentials. In this case, the actual chained CVSS score would be 9.9 - CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H.

## Vendor Response

The vendor has updated their website and uploaded the latest firmware on it. https://inhandnetworks.com/product-security-advisories.html https://www.inhandnetworks.com/products/inrouter300.html#link4

https://www.inhandnetworks.com/upload/attachment/202205/10/InHand-PSA-2022-01.pdf

## Timeline

2022-03-15 - Vendor Disclosure
2022-05-10 - Public Release
2022-05-10 - Vendor Patch Release

## CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.

---