Talos Vulnerability Report

TALOS-2022-1477

InHand Networks InRouter302 console inhand command execution vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-25995

Summary

A command execution vulnerability exists in the console inhand functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.

Tested Versions

InHand Networks InRouter302 V3.5.4

Product URLs

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

CVSSv3 Score

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

CWE

CWE-489 - Leftover Debug Code

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 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>
```

A low-privileged user can login into this service. The Router console contains a command, called `inhand`, that is not listed among the available functionalities. This is probably a leftover debug code. This functionality will request for a password, and based on the value provided, different actions are performed. The `inhand_functionality`:

```
undefined4 inhand_functionality(undefined4 param_1,char *password)
{
  [...]
  if ((password == (char *)0x0) || (*password == '\0')) {
    password = stack_password;
    input_pass_message = get_help_string("input_pass");
    get_pass_wrap(input_pass_message,password,0x40);
  }
  aes_decrypt_str(<REDACTED>,0x40,decrypted_string
                  ,0x40);
[1]
  [...]
  is_correct = strcmp(password,decrypted_string);
[2]
  if (is_correct == 0) {
    alarm(0);
    execl("/bin/sh","sh",0);
[3]
    return 0;
  }
  [...]
} This function will first, at `[1]`, decrypt a hard-coded hex encoded string. Then,
if the comparison between the password at `[2]` returns zero, meaning the two string
are equal, then the code at `[3]` will be reached. Then a `/bin/sh` shell is
provided.
```

The `aes_decrypt_str`:

```
undefined4 aes_decrypt_str(char *data,uint data_len,char *output_buff)
{
  [...]
  IV._0_4_ = 0;
  IV._4_4_ = 0;
  IV._8_4_ = 0;
  IV._12_4_ = 0;
  if ((data_len & 0x1f) == 0) {
    __size = (int)data_len / 2;
    data_bin = malloc(__size);
    if (data_bin == (void *)0x0) {
      syslog(3,"out of memory!");
      uVar1 = 0xffffffff;
    }
    else {
      str2bin(data,__size,data_bin);
      AES_set_key(AES_key,<REDACTED>,128);
[4]
      uVar1 = IH_AES_cbc_encrypt(AES_key,data_bin,output_buff,__size,IV,0);
      free(data_bin);
    }
  }
  [...]
}
```

The hard-coded data provided at `[1]` are decrypted using AES with a hard-coded key, seen at `[4]`. An attacker, in possession of low-privileged user credentials, would be able to obtain a `/bin/sh` shell to the router.

Exploit Proof of Concept

Using the `inhand` command and providing the correct password will prompt a `/bin/sh` shell:

```
Router> inhand
input password:


BusyBox v1.26.2 (2020-10-14 18:29:02 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/www #
```

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

2022-03-16 - Vendor Disclosure

2022-05-10 - Public Release

2022-05-10 - Vendor Patch Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.
