Talos Vulnerability Report

TALOS-2022-1496

InHand Networks InRouter302 console infactory hard-coded password vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-27172

Summary

A hard-coded password vulnerability exists in the console infactory functionality of InHand Networks InRouter302 V3.5.37. A specially-crafted network request can lead to privileged operation execution. An attacker can send a sequence of requests to trigger this vulnerability.

Tested Versions

InHand Networks InRouter302 V3.5.37

Product URLs

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

CVSSv3 Score

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

CWE

CWE-259 - Use of Hard-coded Password

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.

```
***********************************************
           Welcome to Router console
      Inhand
      Copyright @2001-2020, Beijing InHand Networks Co., Ltd.
      http://www.inhandnetworks.com
-----------------------------------------------
Model                : IR302-WLAN
Serial Number        : RF3022141057203
Description          : www.inhandnetworks.com
Current Version      : V3.5.37
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
  infactory      -- factory mode
Router>
```

A low-privileged user can login into this service. The Router console contains a command, called `infactory`. This functionality will request a password; if correct, a menu with several functions is accessed.

The `infactory_command`:

```
undefined4 infactory_command(undefined4 param_1,char *provided_password)

{
 [...]

  if ((provided_password == (char *)0x0) || (*provided_password == '\0')) {
    provided_password = password_in_stack;
    uVar2 = get_help_string("input_pass");
    get_pass_wrap(uVar2,provided_password,0x40);
  }
  aes_decrypt_str(<REDACTED>,0x40,decrypted_password,0x80);
[1]
  password_len = strlen(decrypted_password);
  iVar1 = strncmp(decrypted_password,provided_password,password_len);
[2]
  if (iVar1 == 0) {
    change_view(view_cursor,&view_infactory);
[3]
    return 0;
  }
  [...]
}
```

This function will first, at `[1]`, decrypt a hard-coded hex encoded string. Then, if the comparison between the described string and the provided password, at `[2]`, returns zero, meaning the two string are equal, then the code at `[3]` will be reached. Then the “view” will be changed, which means that the available commands will change.

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, at `[4]`, using AES with a hard-coded key. An attacker, in possession of low-privileged user credentials, would be able to access the `infactory` functionalities.

Exploit Proof of Concept

Using the `infactory` command and providing the correct password will list the `infactory` functionalities:

```
Router> infactory
input password:
Router(factory)#
get help for commands
-----------------------------------------------
type '?' for detail help at any point
===============================================
  help           -- get help for commands
  language       -- Set language
  exit           -- exit current mode/console
  reboot         -- reboot system
  factory-model  -- hardware model configure
  modem          -- modem test
  reset-key      -- check the status of the reset button
  com            -- detecting serial ports
  port           -- FCT network port test
  net            -- complete machine network port test
  led            -- LED lights test
  wlan           -- Wi-Fi test
  mem            -- check memory
  hw_wdg         -- check the hardware watchdog status
  dio            -- detect digital I/O
  stategridsec   -- detect stategrid security chip
Router(factory)#
```

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

2022-03-28 - Vendor Disclosure

2022-05-10 - Public Release

2022-05-10 - Vendor Patch Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.