Talos Vulnerability Report

TALOS-2022-1518

InHand Networks InRouter302 console nvram leftover debug code vulnerability

OCTOBER 27, 2022

CVE NUMBER

CVE-2022-29481

SUMMARY

A leftover debug code vulnerability exists in the console nvram functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted series of network requests can lead to disabling security features. An attacker can send a sequence of requests to trigger this vulnerability.

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

InHand Networks InRouter302 V3.5.45

PRODUCT URLS

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

CVSSV3 SCORE

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

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 @2001-2022, Beijing InHand Networks Co., Ltd.
      http://www.inhandnetworks.com
----------------------------------------------
Model                : IR302-WLAN
Serial Number        : RF3022141057203
Description          : www.inhandnetworks.com
Current Version      : V3.5.45
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, after providing 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 `configure`. This command allows users to enter the configuration mode and modify several configurations:

```
Router# configure terminal
Router(config)#
get help for commands
-----------------------------------------------
type '?' for detail help at any point
===============================================
  help           -- get help for commands
  language       -- Set language
  clock          -- set system date and time
  ntp            -- set network time service
  show           -- show system information
  config         -- configuration
  exit           -- exit current mode/console
  reboot         -- reboot system
  hostname       -- set host name
  ping           -- ping test
  comredirect    -- COM redirector
  telnet         -- telnet to a host
  traceroute     -- trace route to a host
  enable         -- change enable password
  disable        -- turn off privileged commands
  username       -- set username and password
  no             -- unset the given argument
  default        -- reset the given argument to default value
```

In the `configure` view there is a command, called `nvram`, that is not listed among the available functions. This is probably a leftover debug code:

```
Router(config)# nvram
nvram operation
================================================
Arguments:
  get <name>     -- get var
  set <name> [<value>]
                 -- set var
  commit
Router(config)#
```

It is possible to obtain and set any nvram variable. For instance, it would be possible to disable the firmware signature verification flag and upload a malicious firmware to the device. This vulnerability can enable advisories TALOS-2022-1477, TALOS-2022-1495 and TALOS-2022-1496 again.

Exploit Proof of Concept

Here is an example of setting a key value pair using the hidden functionalities:

```
Router(config)# nvram set key value
%WARNING: key=value is invalid!
Router(config)#
```

Even if it says ` %WARNING: key=value is invalid!` the value is set nevertheless. The same command would work for critical nvram keys.

TIMELINE

2022-06-07 - Vendor Disclosure
2022-10-25 - Vendor Patch Release
2022-10-27 - Public Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.
