Talos Vulnerability Report

TALOS-2022-1520

InHand Networks InRouter302 console verify leftover debug code vulnerability

OCTOBER 27, 2022

CVE NUMBER

CVE-2022-26023

SUMMARY

A leftover debug code vulnerability exists in the console verify 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

6.5 - CVSS:3.0/AV:N/AC:L/PR:L/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>
```

The Router console contains a command, called `verify`, that is not listed among the available functionalities. This is probably a leftover debug code. This command allows to enable or disable the firmware signature verification, leading to enabling advisory TALOS-2022-1495 again.

Exploit Proof of Concept

The command allows to disable the firmware signature verification, specifying disable as argument:

```
Router> verify
0*wveriP�)w
================================================
Arguments:
  enable
  disable
Router> verify disable
```

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.

VULNERABILITY REPORTS

PREVIOUS REPORT

NEXT REPORT

TALOS-2022-1518

TALOS-2022-1521