Talos Vulnerability Report

TALOS-2022-1474

InHand Networks InRouter302 router configuration export information disclosure vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-26020

Summary

An information disclosure vulnerability exists in the router configuration export functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted network request can lead to increased privileges. An attacker can send an HTTP request to trigger this vulnerability.

Tested Versions

InHand Networks InRouter302 V3.5.4

Product URLs

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

CVSSv3 Score

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

CWE

CWE-321 - Use of Hard-coded Cryptographic Key

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 several functionalities where the secrecy of the data is essential. But the majority of data are saved into the nvram configuration file, which is downloadable by any logged-in users. For this reason, some of the nvram entries are encrypted. The function that encrypt the entry value is `aes_encrypt_str`:

```
undefined4 aes_encrypt_str(char *data_in,int len,char *data_out)

{
  [...]
  IV._0_4_ = 0;
  __size = len + 0xfU & 0xfffffff0;
  IV._4_4_ = 0;
  IV._8_4_ = 0;
  IV._12_4_ = 0;
  data_in_copy = crypto_dup(data_in,len,__size);
  if (data_in_copy == 0) {
    uVar1 = 0xffffffff;
  }
  else {
    data_out_temp = malloc(__size);
    if (data_out_temp == (void *)0x0) {
      [...]
    }
    else {
      AES_set_key(AES_key,<REDACTED>,0x80);
[1]
      uVar1 = IH_AES_cbc_encrypt(AES_key,data_in_copy,data_out_temp,__size,IV,1);
[2]
      bin2str(data_out_temp,__size,data_out);
      free(data_in_copy);
      free(data_out_temp);
    }
  }
  return uVar1;
}
```

The `aes_encrypt_str` function sets the AES key at `[1]` and then encrypts the provided string at `[2]`. The AES key at `[1]` is hard-coded. An attacker that is able to obtain the encrypted string could use the AES key at `[1]` to decrypt those.

Exploit Proof of Concept

Following the request to download the nvram configuration file:

```
GET /config.dat?type=config HTTP/1.1
Host: 192.168.2.1
Cookie: web_session=2edc3370
Connection: close
```

The router reply will be:

```
HTTP/1.0 200 OK
Date: Mon, 06 Jul 2020 12:16:42 GMT
Content-Type: application/octent-stream
Cache-Control: no-cache, no-store, must-revalidate, private
Expires: Thu, 31 Dec 1970 00:00:00 GMT
Pragma: no-cache
Connection: close

#BEGIN-CONFIG TIMESTAMP:1594037762
[...]
adm_passwd=$AES$664C98C2428A8DA4B7E39345A8E29967
adm_user=adm
adm_users=$AES$7453839E7CEBBFF515F60FAB57781B45
[...]
cert_private=$AES$2EDA91DB0EB549AD1B6DBB[...]
cert_key=$AES$73E3FEF28D45C1CD652FECE871B7C624
[...]
```

For instance, we can see that: `adm_passwd`, `adm_users`, `cert_private` and `cert_key` are nvram entries with AES-encrypted values. A low-privileged user could download the configuration file and get this information. For instance, one consequence would be for a low-privileged user to obtain the privileged user credentials.

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

2022-03-02 - Vendor Disclosure
2022-05-10 - Public Release
2022-05-10 - Vendor Patch Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2022-1473

NEXT REPORT

TALOS-2022-1475