Talos Vulnerability Report

TALOS-2022-1473

InHand Networks InRouter302 httpd wlscan_ASP OS command injection vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-26085

Summary

An OS command injection vulnerability exists in the httpd wlscan_ASP functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated 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

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 uses, inside its HTML pages, a minimal template language. The symbols between <% and %> are parsed server-side. For instance, the string <% wlscan(); %>, inside an HTML page, will call the httpd's wlscan_ASP function. The output generated will be embedded in the original HTML page, replacing the template token. The wlscan_ASP:

```
void wlscan_ASP(void)
{

      wl0_ap_ptr = (char *)nvram_safe_get("wl0_ap");
[1]
      wl0_ap_value = atoi(wl0_ap_ptr);
      [...]
      wl0_iface_nvram_ptr = nvram_safe_get("wl0_iface");
      snprintf(wl0_iface,0xc,"%s",wl0_iface_nvram_ptr);
[2]
      if (wl0_ap_value == 0) {
        stack_buf_ptr = stack_buf;
        wl0_iface_nvram_ptr = nvram_safe_get("wl0_ssid");
        strlcpy(stack_buf_ptr,wl0_iface_nvram_ptr,0x40);
        sprintf((char *)&command_line,"iwpriv %s connStatus",wl0_iface);
[3]
        popen_res = popen((char *)&command_line,"r");
[4]
      }

[...]
}
```

At [2] 0xc characters of the string wl0_iface, extracted from the nvram, are placed into a buffer. If the value of the wl0_ap variable, extracted at [1] from the nvram, is zero, then the code at [4] and [5] are reached. At [4], the string iwpriv <wl0_iface> connStatus is generated. This string will then pass, at [5], through popen to obtain the information of the connStatus private-command of the <wl0_iface>. As soon as one HTML page with the <% wlscan(); %> token is requested, by a logged-in user, the wlscan_ASP function will be reached.

Controlling wl0_ap and wl0_iface would lead to a command injection at [4].

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

2022-02-25 - Initial vendor contact

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 | NEXT REPORT

TALOS-2022-1472 | TALOS-2022-1474