Talos Vulnerability Report

TALOS-2022-1571

Robustel R1510 web_server /action/remove/ API data removal vulnerability

JUNE 30, 2022

CVE NUMBER

CVE-2022-28127

Summary

A data removal vulnerability exists in the web_server /action/remove/ API functionality of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary file deletion. An attacker can send a sequence of requests to trigger this vulnerability.

Tested Versions

Robustel R1510 3.3.0

Product URLs

R1510 - https://www.robustel.com/en/product/r1510-industrial-cellular-vpn-router/

CVSSv3 Score

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

CWE

CWE-20 - Improper Input Validation

Details

The R1510 is an industrial cellular router. It offers several advanced software like an innovative use of Open VPN, Cloud management, data over-use guard, smart reboot and others.

The R1510 has a web server that manages several APIs. One of these API is `/ajax/remove/`. This function allows to remove files, checking for possible path traversal in the provided input.

Here it is the function that handles the `/ajax/remove/` API:

```
undefined4 /ajax/remove/(Webs *webs)

{
  [...]

  [...]
      file_name = (char *)websGetVar(webs,"file_name",0);
[1]
      if ((file_name != (char *)0x0) &&
         (shell_command = strstr(file_name,".."), shell_command == (char *)0x0)) {
[2]
        shell_command = (char *)sfmt("rm %s -rf",file_name);
[3]
        iVar1 = system(shell_command);
        [...]
}
```

At `[1]` the variable `file_name` is fetched and then used, at `[3]`, to create the string `rm <file_name> -rf`. The function checks, at `[2]`, if the provided `filen_name` contains `..`. This check, allegedly, is used to prevent path traversal. But because `file_name` can be an absolute path, an attacker, able to control `file_name` would be able to delete arbitrary file and directory.

Timeline

2022-06-27 - Initial vendor contact

2022-06-28 - Vendor Disclosure

2022-06-30 - Public Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.

VULNERABILITY REPORTS PREVIOUS REPORT NEXT REPORT

TALOS-2022-1572 TALOS-2022-1570