Talos Vulnerability Report

TALOS-2022-1580

Robustel R1510 sysupgrade firmware update vulnerability

OCTOBER 14, 2022

CVE NUMBER

CVE-2022-34845

SUMMARY

A firmware update vulnerability exists in the sysupgrade functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network packet can lead to arbitrary firmware update. 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.

Robustel R1510 3.1.16
Robustel R1510 3.3.0

PRODUCT URLS

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

CVSSV3 SCORE

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

CWE

CWE-345 - Insufficient Verification of Data Authenticity

DETAILS

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

The R1510 offers to the admin user the possibility of upgrading the firmware. The API `/action/import_firmware` is used to upload the firmware file. Then the `/ajax/system_upgrade_start/` API can be called. This function, eventually, will call the `sysupgrade` binary that will perform the actual firmware upgrade.

Here is the relevant portion of the `/ajax/system_upgrade_start/` API:

```
[...]
{
    command[0] = "sysupgrade";
    command[1] = "-q";
    command[2] = FILENAME;
    command[3] = 0;
    void var_18;
    _eval(command, 0, 0, &pid);
}
[...]
```

The `/ajax/system_upgrade_start/` API is a wrapper for executing `sysupgrade -q <FILENAME>`. The `FILENAME` variable is set in the `/action/import_firmware` and has as value the pathname to the firmware file. The `sysupgrade` will perform the firmware upgrade, but with the current settings the binary does not check for any signature verification. This can lead to arbitrary firmware update.

TIMELINE

2022-07-13 - Vendor Disclosure
2022-10-14 - Public Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.
