Talos Vulnerability Report

TALOS-2022-1576

Robustel R1510 sysupgrade command injection OS command injection vulnerability

OCTOBER 14, 2022

CVE NUMBER

CVE-2022-32765

SUMMARY

An OS command injection vulnerability exists in the sysupgrade command injection functionality of Robustel R1510 3.1.16 and 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.

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

9.1 - CVSS:3.0/AV:N/AC:L/PR:H/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 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. A specific API is called for uploading the new firmware, then the `sysupgrade` binary is called:

```
int sysupgrade(int argc,char **argv)
{
  [...]
  upgrade_magic = sysupgrade_is_valid_header(upgrade_filepath);
  if (upgrade_magic == 0x726f7324) {
    [...]
    else if (!IS_REMOVE_AND_SAVE_HEADER) {
      [...]
      upgrade_obj_ = (char *)&upgrade_obj;
      current_option_number = fw_check_size(upgrade_filepath,upgrade_obj_);
      [... various check and parsing functions ...]
      if (upgrade_obj.type != 6) {
        if (upgrade_obj.type == 7) {
          [...]
          current_pid = getpid();
          snprintf(&RPK_PATHNAME,
                   0x1000,"/tmp/sysupgrade/%d-
%s.rpk",current_pid,upgrade_obj.file_desc);               [1]
        [...]
        goto CONTINUE_UPDATE;
      [...]
  CONTINUE_UPDATE:
      [...]
      shell_cmd = "rpkg install %s";
      goto EXECUTE_SHELL_CMD;
      [...]
  EXECUTE_SHELL_CMD:
      current_option = sysprintf(shell_cmd,&RPK_PATHNAME);
[2]
      [...]
}
```

The binary will parse and perform validation checks over the provided file. A precisely-crafted upgrade file can make the `sysupgrade` binary reach the code at `[1]`. The `snprintf` instruction at `[1]` will create the `RPK_PATHNAME` variable using the provided `upgrade_obj.file_desc`. Then at `[2]`the format string `rpkg install %s` is used as first argument of the `sysprintf` function and `RPK_PATHNAME` as the second one.

Here is the `sysprintf` function:

```
void sysprintf(char *format_string,char *param_2,char *char*,char *param_4)

{
  [...]

  va_list_ptr = va_list;
  va_list[0] = param_2;
  va_list[1] = char*;
  va_list[2] = param_4;
  vsnprintf(shell_command,0x200,format_string,va_list_ptr);
[3]
  system(shell_command);
[4]
  return;
}
```

At `[3]` a string is formatted, using the first argument of the function as format string and the other parameters as format string arguments. If one of the arguments is controllable by an attacker, a command injection would occur at `[4]`. Because the `upgrade_obj.file_desc` is not checked against command injections, the instruction at `[4]` can lead to a command injection.

TIMELINE

2022-07-13 - Vendor Disclosure

2022-10-14 - Public Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

NEXT REPORT

TALOS-2022-1575

TALOS-2022-1579