Talos Vulnerability Report

TALOS-2021-1422

Reolink RLC-410W cgiserver.cgi Upgrade API denial of service vulnerability

JANUARY 26, 2022

CVE NUMBER

CVE-2021-40405

Summary

A denial of service vulnerability exists in the cgiserver.cgi Upgrade API functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. An attacker can send an HTTP request to trigger this vulnerability.

Tested Versions

Reolink RLC-410W v3.0.0.136_20121102

Product URLs

RLC-410W - https://reolink.com/us/product/rlc-410w/

CVSSv3 Score

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

CWE

CWE-284 - Improper Access Control

Details

The Reolink RLC-410W is a WiFi security camera. The camera includes motion detection functionalities and various methods to save the recordings.

The RLC-410W offers different APIs for different levels of authentication. One of these APIs reboots the device. This API should be executed by administrator users only.

A specially-crafted HTTP request can kill the `cgiserver.cgi` process and lead to the reboot of the device, without the required permission.

The `cgiserver.cgi` checks if a user has the permission to perform a certain action in the API functionality itself. For instance, for the `Upgrade` API we have the following instructions at the beginning of the code:

```
undefined4 Upgrade(cgi_session *session,cgi_cmd *cmd)

{
    [...]

    if (cmd->parsing_status == NOT_HANDLED) {
        error_code = cgi_check_ability(cmd->command_ID,session,0);                                    [1]
        if (error_code != NO error) {
        cgi_log(1,0,"[%s,%d]",
                "/home/lgb/ipc_v1_ver/20201211/ipc_20200324_V1/product/cgiserver/src/cgi_system.cpp",
                0xf1e);
        cgi_log(0,0,"cmd%d, cgi_check_abiliby failed! [need reboot]",cmd->command_ID);
        cmd->HTTP_status_code = error_code;
        cmd->associated_request->perform_reboot = 1;                                                  [2]
        return 0xffffffff;
        }
        cmd->parsing_status = PARSE_OK;
    }
[...]
}
```

At `[1]` the permission of the user is checked against the permission of the required API, `Upgrade` in this specific case. This prohibits the execution of certain APIs for non-authorized users. But in the specific case of `Upgrade`, if the permission check fails, the device will set, at `[2]`, the `perform_reboot` flag and the device will reboot, essentially allowing a non-authorized user to perform the reboot operation.

Note that, while this issue requires a logged-in user, it's possible to use TALOS-2021-1420 to perform this API call without authentication. In this case, the actual chained CVSS score would be 8.6 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H.

Timeline

2021-12-06 - Vendor Disclosure
2022-01-19 - Vendor Patched
2022-01-26 - Public Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.