```
RCE Security Advisory
https://www.rcesecurity.com


1. ADVISORY INFORMATION
=======================
Product:        Reolink E1 Zoom Camera
Vendor URL:     https://reolink.com/product/e1-zoom/
Type:           Exposure of Sensitive Information to an Unauthorized Actor [CWE-200]
Date found:     2021-08-26
Date published: 2022-06-01
CVSSv3 Score:   5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CVE:            CVE-2021-40150


2. CREDITS
==========
This vulnerability was discovered and researched by Julien Ahrens from
RCE Security.


3. VERSIONS AFFECTED
====================
Reolink E1 Zoom Camera 3.0.0.716 (latest) and below


4. INTRODUCTION
===============
Meet new generation of Reolink E1 series. Advanced features - 5MP Super HD
& optical zoom are added into this compact camera. Plus two-way audio, remote
live view and more smart capacities help you connect with what you care. Be
closer to families and be away from worries.

(from the vendor's homepage)


5. VULNERABILITY DETAILS
========================
The web server of the E1 Zoom camera through 3.0.0.716 discloses its configuration
via the /conf/ directory that is mapped to a publicly accessible path.

An unauthenticated attacker can abuse this with network-level access to
the camera to download the entire NGINX/FastCGI configurations by querying, i.e.:

http://[CAM-IP]/conf/nginx.conf
http://[CAM-IP]/conf/fastcgi.conf

Etc.


6. RISK
=======
An unauthenticated attacker can download the webserver's configuration
files which might lead to sensitive information disclosure.


7. SOLUTION
===========
None.


8. REPORT TIMELINE
==================
2021-08-26: Discovery of the vulnerability
2021-08-26: Sent notification to Reolink via their support channel
2021-08-26: Response from vendor asking for vulnerability details
2021-08-26: Sent all the vulnerability details
2021-08-31: Vendor is still looking into the issue
2021-09-03: Vendor states that the issue will be fixed with the next firmware update by the end of September.
2021-10-01: Since no firmware has been released, we've sent another notification
2021-10-02: Vendor states that the new firmware is delayed
2022-02-01: Since there is still fix, sent another notification
2022-02-02: Vendor states that the firmware with the fix hasn't been released yet.
2022-03-03: Since there is still fix, sent another notification
2022-03-12: Vendor states they're still working on the issue (internal update awaits testing)
2022-05-24: Since there is still fix, sent another notification
2022-05-24: Vendor states that the update still hasn't been released yet.
2022-06-01: Almost a year should be enough to fix this. Public disclosure.
```

```
79
80
81 9. REFERENCES
82 =============
83 https://github.com/MrTuxracer/advisories
```