Reolink E1 Zoom Camera 3.0.0.716 Private Key Disclosure

Authored by Julien Ahrens | Site rcesecurity.com

Posted Jun 6, 2022

Reolink E1 Zoom Camera versions 3.0.0.716 and below suffer from a private key disclosure vulnerability.

tags | exploit, info disclosure
advisories | CVE-2021-40149
SHA-256 | 6a0bd039c1f58f660697b01a27d1512dbd2ffb57a9229991176f80a78cd66c64 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
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:   7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
CVE:            CVE-2021-40149


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 SSL private
key via the root web server directory.

An unauthenticated attacker can abuse this with network-level access to the
camera to download the webserver's private SSL key by simply going to the
following URL:

http://[CAM-IP]/self.key


6. RISK
=======
An unauthenticated attacker can download the webserver's SSL private key and
thereby attack the encrypted network traffic to and from the camera, which might
lead to the disclosure of the administrative access credentials and other
sensitive information.


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 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.


9. REFERENCES
=============
https://github.com/MrTuxracer/advisories
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed