



CVE-2021-40407

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-40407
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-28 20:15:00 UTC
Updated	2022-07-29 15:25:00 UTC
Description	An OS command injection vulnerability exists in the device network settings functionality of reolink RLC-410W v3.0.0.136_2

Risk And Classification

EPSS: 0.325750000 probability, percentile 0.968410000 (date 2026-04-02)

CISA KEV: Listed on 2024-12-18; due 2025-01-08; ransomware use Unknown

Problem Types: CWE-78

CISA Known Exploited Vulnerability

Vendor	Reolink
Product	RLC-410W IP Camera
Name	Reolink RLC-410W IP Camera OS Command Injection Vulnerability
Required Action	The impacted product could be end-of-life (EoL) and/or end-of-service (EoS). Users should discontinue product utilization if a current mitigation is unavailable.
Notes	https://reolink.com/product-eol/ ; https://reolink.com/download-center/ ; https://nvd.nist.gov/vuln/detail/CVE-2021-40407

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Reolink	Rlc-410w	-	All	All	All
Operating System	Reolink	Rlc-410w Firmware	3.0.0.136_20121102	All	All	All

References

Reference	Source	Link	Tags
TALOS-2021-1424 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

591049 Reolink RLC-410W device network settings OS command injection Multiple Vulnerabilities (TALOS-2021-1424)

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

CVE.report and Source URL Uptime Status status.cve.report