

CVE-2021-40407

Reolink RLC-410W IP Camera OS Command Injection Vulnerability

CISA KEV since Dec 18, 2024

Actively exploited

An OS command injection vulnerability exists in the device network settings functionality of reolink RLC-410W v3.0.0.136_20121102. At [1] or [2], based on DDNS type, the ddns->domain variable, that has the value of the domain parameter provided through the SetDdns API, is not validated properly. This would lead to an OS command injection. An attacker can send an HTTP request to trigger this vulnerability.

EVRS 75/100 Urgent priority	CVSS V3.1 7.2 High · NVD	EPSS 0.476 98.8th percentile · FIRST	CISA DEADLINE Jan 8, 2025 KEV since 2024 · listed over a year
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.476 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA 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.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
rlc-410w firmware	3.0.0.136_20121102	no fixed version listed	NVD
rlc-410w	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-3w42-xvww-qc2q	reolink.com	reolink.com/product-eol/
reolink.com	reolink.com/download-center/	NVD	nvd.nist.gov/vuln/detail/CVE-2021-40407
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-27584
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-40407		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.