



# CVE-2022-21801

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-21801
<b>State</b>	PUBLIC
<b>Assigner</b>	talos-cna@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-01-28 20:15:00 UTC
<b>Updated</b>	2022-07-01 19:17:00 UTC
<b>Description</b>	A denial of service vulnerability exists in the netserver recv_command functionality of reolink RLC-410W v3.0.0.136_20121

## Risk And Classification

**Problem Types:** CWE-190

## 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 Website	MISC	<a href="https://talosintelligence.com">talosintelligence.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

591159 Reolink RLC-410W netserver recv\_command Denial of Service (DoS) Vulnerability (TALOS-2022-1450)

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**