



# CVE-2021-40404

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

## Summary

<b>CVE</b>	CVE-2021-40404
<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>	2022-08-09 00:40:00 UTC
<b>Description</b>	An authentication bypass vulnerability exists in the cgiserver.cgi Login functionality of reolink RLC-410W v3.0.0.136_20121

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Reolink</a>	<a href="#">Rlc-410w</a>	-	All	All	All
Operating System	<a href="#">Reolink</a>	<a href="#">Rlc-410w Firmware</a>	3.0.0.136_20121102	All	All	All

## References

Reference	Source	Link	Tags
TALOS-2021-1420    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	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, ar

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[591209](#) Reolink RLC-410W cgiserver.cgi Login authentication bypass Vulnerability (TALOS-2021-1420)

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](#) 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](#)**