CVE-2021-40404

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-40404
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	2022-08-09 00:40:00 UTC
Description	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	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-2021-1420 || 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

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)

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