



CVE-2021-33219

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-33219
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-07 15:15:00 UTC
Updated	2021-07-09 16:51:00 UTC
Description	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Hard-coded Web Application

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Commscope	Ruckus lot Controller	All	All	All	All

References

Reference	Source	L
KoreLogic - Advisories	MISC	k
Full Disclosure: KL-001-2021-004: CommScope Ruckus IoT Controller Hard-coded Web Application Administrator Password	MISC	s
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)