CVE-2021-33221

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-33221
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 16:44:00 UTC
Description	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Unauthenticated API Endpoi

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
KoreLogic - Advisories	MISC	korelogic.com	
Full Disclosure: KL-001-2021-001: CommScope Ruckus IoT Controller Unauthenticated API Endpoints	MISC	seclists.org	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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

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