



CVE-2021-33217

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

Summary

CVE	CVE-2021-33217
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 16:52:00 UTC
Description	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. The Web Application allows Arbitrary R

Risk And Classification

Problem Types: CWE-787

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	Link
Full Disclosure: KL-001-2021-006: CommScope Ruckus IoT Controller Web Application Arbitrary Read/Write	MISC	seclists.org
KoreLogic - Advisories	MISC	korelogic.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)