



# CVE-2021-33215

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

## Summary

<b>CVE</b>	CVE-2021-33215
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-07-07 15:15:00 UTC
<b>Updated</b>	2021-07-09 16:48:00 UTC
<b>Description</b>	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. The API allows Directory Traversal.

## Risk And Classification

**Problem Types:** CWE-22

## 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	Ta
Full Disclosure: KL-001-2021-005: CommScope Ruckus IoT Controller Web Application Directory Traversal	MISC	<a href="https://seclists.org">seclists.org</a>	
KoreLogic - Advisories	MISC	<a href="https://korelogic.com">korelogic.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

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](#)**