Ruckus AP CLI Arbitrary File Read Allows Authenticated Remote File Access

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-4474
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 20:16:07 UTC
Updated	2026-03-30 13:26:50 UTC
Description	Ruckus Access Point products contain an arbitrary file read vulnerability in the command-line interface that allows authentic

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000510000 probability, percentile 0.157610000 (date 2026-04-02)

Problem Types: CWE-552 | CWE-552 CWE-552 Files or Directories Accessible to External Parties

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/S/
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/S/
3.1	disclosure@vulncheck.com	Primary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ruckus Wireless	RUCKUS Access Point	affected semver	Not specified
CNA	Ruckus	RUCKUS Unleashed	affected semver	Not specified

CNA	Ruckus	SmartZone 100 SZ-100 EOL	affected semver	Not specified
CNA	Ruckus	SmartZone 100-D SZ100-D EOL	affected semver	Not specified
CNA	Ruckus	SmartZone 144 SZ-144	affected semver	Not specified
CNA	Ruckus	SmartZone 144-Dataplane SZ144-D	affected semver	Not specified
CNA	Ruckus	SmartZone 300 SZ300 EOL	affected semver	Not specified
CNA	Ruckus	ZoneDirector 1200 EOL	affected semver	Not specified

References

Reference	Source	Link
www.vulncheck.com/advisories/ruckus-ap-cli-arbitrary-file-read-allows-authentic...	disclosure@vulncheck.com	www.vulncheck.com
support.ruckuswireless.com/security_bulletins/306	disclosure@vulncheck.com	support.ruckuswireless.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.