



# Ruckus AP CLI Arbitrary File Read Allows Authenticated Remote File Access

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

## Summary

<b>CVE</b>	CVE-2021-4474
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 20:16:07 UTC
<b>Updated</b>	2026-03-30 13:26:50 UTC
<b>Description</b>	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/MSX/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/MSG: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	<a href="#">Ruckus</a>	<a href="#">SmartZone 100 SZ-100 EOL</a>	affected semver	Not specified
CNA	<a href="#">Ruckus</a>	<a href="#">SmartZone 100-D SZ100-D EOL</a>	affected semver	Not specified
CNA	<a href="#">Ruckus</a>	<a href="#">SmartZone 144 SZ-144</a>	affected semver	Not specified
CNA	<a href="#">Ruckus</a>	<a href="#">SmartZone 144-Dataplane SZ144-D</a>	affected semver	Not specified
CNA	<a href="#">Ruckus</a>	<a href="#">SmartZone 300 SZ300 EOL</a>	affected semver	Not specified
CNA	<a href="#">Ruckus</a>	<a href="#">ZoneDirector 1200 EOL</a>	affected semver	Not specified

## References

Reference	Source	Link
<a href="http://www.vulncheck.com/advisories/ruckus-ap-cli-arbitrary-file-read-allows-authentic...">www.vulncheck.com/advisories/ruckus-ap-cli-arbitrary-file-read-allows-authentic...</a>	disclosure@vulncheck.com	<a href="http://www.vulncheck.com">www.vulncheck.com</a>
<a href="http://support.ruckuswireless.com/security_bulletins/306">support.ruckuswireless.com/security_bulletins/306</a>	disclosure@vulncheck.com	<a href="http://support.ruckuswireless.com">support.ruckuswireless.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](https://status.cve.report)