



# CVE-2020-22657

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

## Summary

<b>CVE</b>	CVE-2020-22657
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-01-20 19:15:00 UTC
<b>Updated</b>	2023-01-30 18:01:00 UTC
<b>Description</b>	In Ruckus R310 10.5.1.0.199, Ruckus R500 10.5.1.0.199, Ruckus R600 10.5.1.0.199, Ruckus T300 10.5.1.0.199, Ruckus

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Ruckuswireless</a>	R310	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	R310 Firmware	10.5.1.0.199	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	R500	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	R500 Firmware	10.5.1.0.199	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	R600	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	R600 Firmware	10.5.1.0.199	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	Scg200	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	Scg200 Firmware	All	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	Sz-100	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	Sz-100 Firmware	All	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	Sz-300	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	Sz-300 Firmware	All	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	T300	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	T300 Firmware	10.5.1.0.199	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	T301n	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	T301n Firmware	10.5.1.0.199	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	T301s	-	All	All	All

Operating System	<a href="#">Ruckuswireless</a>	<a href="#">T301s Firmware</a>	10.5.1.0.199	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	<a href="#">Vsz</a>	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	<a href="#">Vsz Firmware</a>	All	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	<a href="#">Zonedirector 1100</a>	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	<a href="#">Zonedirector 1100 Firmware</a>	9.10.2.0.130	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	<a href="#">Zonedirector 1200</a>	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	<a href="#">Zonedirector 1200 Firmware</a>	10.2.1.0.218	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	<a href="#">Zonedirector 3000</a>	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	<a href="#">Zonedirector 3000 Firmware</a>	10.2.1.0.218	All	All	All
Hardware	<a href="#">Ruckuswireless</a>	<a href="#">Zonedirector 5000</a>	-	All	All	All
Operating System	<a href="#">Ruckuswireless</a>	<a href="#">Zonedirector 5000 Firmware</a>	10.0.1.0.151	All	All	All

## References

Reference	Source	Link	Tags
20200302   Security Bulletins   Ruckus Wireless Support	MISC	<a href="https://support.ruckuswireless.com">support.ruckuswireless.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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)