

## Security Advisory: ID 20250122

### Multiple vulnerabilities in RUCKUS Unleashed and ZoneDirector

Public Release: Jan 27, 2025

#### What is the issue?

Unleashed APs and ZoneDirector running versions of software indicated below contain a number of critical vulnerabilities. Collectively, these vulnerabilities allow a remote, unauthenticated attacker to gain shell access to the device.

RUCKUS Networks would like to recognize and thank René Ammerlaan for finding and reporting these issues to us.

#### What action should I take?

Updating the software to its most recent version, as detailed below, will resolve the vulnerability. Since these are critical vulnerabilities, all impacted customers are strongly encouraged to apply the update as soon as possible and reset all the credentials.

#### Are there any workarounds available?

There is no workaround for these vulnerabilities. For partial mitigation in ZoneDirector releases prior to 10.5.1.0.279 and Unleashed releases 200.15 and 200.16, it is highly recommended that ftp service on the affected device is turned off via the system configuration CLI command **no ftp**.

Example command sequence:

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# no ftp
```

Unleashed release 200.17, 200.15.6.212.14, and ZoneDirector release 10.5.1.0.279 have mitigations in place to disable File Transfer Protocol (FTP) after upgrade to the release.

#### What is the impact on RUCKUS products?

The following table describes the vulnerable products, software versions, and the recommended actions.

Product	Vulnerable Releases	Resolution	Release Date
Unleashed	<ul style="list-style-type: none"><li>200.15.6.112.54 and previous</li><li>200.16</li></ul>	Upgrade to: <ul style="list-style-type: none"><li>200.15.6.212.14 or later</li><li>200.17.7.0.139 or later</li></ul>	<ul style="list-style-type: none"><li>Dec 11, 2024</li><li>Dec 11, 2024</li></ul>
ZoneDirector	All	Upgrade to 10.5.1.0.279 or later	Jan 18, 2025

## When will this RUCKUS Security Advisory be publicly posted?

RUCKUS released the initial security advisory to RUCKUS field teams on: Jan 03, 2025

RUCKUS released the initial security advisory to customers on: Jan 22, 2025

Public posting: Jan 27, 2025

## Revision History

Version	ID	Change	Date
1.0	20250122	Initial Release	Jan 22, 2025

## RUCKUS Support

The RUCKUS Customer Services & Support organization can be contacted via phone, chat, and through our web portal. Details at <https://support.ruckuswireless.com/contact-us>.

© 2025 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates.

("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

### Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS, SOFTWARE, AND/OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMScope DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

### Limitation of Liability

IN NO EVENT SHALL COMMScope, COMMScope AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMScope HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

### Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgellon, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.