

Security Advisory: ID 20210719

RUCKUS SmartZone Reflective Amplification Attack Vulnerability

Internal Release Date: **07/19/2021**

Public Release: **07/19/2021**

What is the issue?

A vulnerability in the eAut module of RUCKUS SmartZone Controller could allow an unauthenticated, remote attacker to perform a DoS attack against another network device by sending a crafted request to the vulnerable module.

This vulnerability is due to an improper handling of an error condition. This causes the vulnerable module to send a UDP packet of 5288 bytes in size.

RUCKUS would like to recognize and thank Li-Xiang, Baidu security researcher, and Borja Marcos from Sarnet for finding and reporting this issue to us.

What action should I take?

RUCKUS is releasing the fix for these vulnerability through a software update. Since it is a severe issue, all affected customers are strongly encouraged to apply the fix once available.

In case of any questions contact RUCKUS TAC through regular means as described at <https://support.ruckuswireless.com/contact-us> and refer to this document to validate this entitlement.

Are there any workarounds available?

Blocking port 9001 using firewall can mitigate this vulnerability.

What is the impact on Ruckus products?

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

| Product | Vulnerable Release | Resolution | Release Date |
|-----------|--------------------|--------------------------|--------------|
| SmartZone | 3.6.2 and earlier | Contact Customer Support | 7/16/21 |

It should be noted that this vulnerability applies to both SmartZone and virtual SmartZone.

When will this RUCKUS Security Advisory be publicly posted?

RUCKUS released the initial security advisory to RUCKUS field teams on: 07/19/2021

RUCKUS released the initial security advisory to customers on: 07/19/2021

Public posting: 07/19/2021

Revision History

| Version | ID | Change | Date |
|---------|----------|-----------------|---------------|
| 1.0 | 20210719 | Initial Release | July 19, 2021 |

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>.

© 2021 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.