Security Advisory: ID 20250710

Reported vulnerabilities in RUCKUS SmartZone and RUCKUS Network Director: CVE-2025-44957, CVE-2025-44962, CVE-2025-44960, CVE-2025-44961, CVE-2025-44963, CVE-2025-44955, CVE-2025-6243, CVE-2025-44958

Public Release: **July 10, 2025**

What is the issue?
It has been reported by CERT/CC that RUCKUS SmartZone Controller (SZ) and RUCKUS Network Director (RND) contain a number of critical vulnerabilities. If exploited, these vulnerabilities allow a remote, unauthenticated attacker to gain shell access to the affected device.

RUCKUS is actively working on the fix and will provide updates as new information becomes available.

RUCKUS would like to recognize Noam Moshe of Claroty Team82 for his research.

What action should I take?
Please monitor this advisory for updates. RUCKUS will publish software fixes once available. Customers are strongly encouraged to upgrade their systems as soon as a patch is released.

Are there any workarounds available?
To reduce exposure, RUCKUS recommends the following mitigations while it continues to investigate:

1. Deploy SZ and RND in accordance with best security practices:
    a. https://support.ruckuswireless.com/security_bulletins/278
2. Restrict network access to potentially vulnerable devices to a limited set of trusted users.

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
SmartZone	All	Apply KSP or upgrade to: • 6.1.2.p3 KSP (SecurityFix_6_1_2_487-15389-v1_0c5006774d7.ksp) • 7.1 KSP (SecurityFix_7_1_0_0_586-15389-v1_1141f30a5b6.ksp) • 5.2.2 KSP (SecurityFix_5_2_2_0_1563-15389-v1_866974.ksp) • 5.2.1.3 KSP (SecurityFix_5_2_1_3_1563-15389-v1_866985.ksp) • 6.1.2p3 Refresh Build	• July 15, 2025 • July 18, 2025 • July 21, 2025 • July 23, 2025 • July 25, 2025
Network Director	All	Upgrade to: • 3.0 • 4.0 • 4.5	• July 15, 2025 • July 18, 2025 • July 21, 2025

If you already have KSP applied in your SZ, please contact RUCKUS support team to avoid possible KSP conflicts.

When will this RUCKUS Security Advisory be publicly posted?

RUCKUS released the initial security advisory to RUCKUS field teams on: July 10, 2025

RUCKUS released the initial security advisory to customers on: July 10, 2025

Public posting: July 10, 2025

Revision History

Version	ID	Change	Date
1.0	20250710	Initial Release	July 10, 2025
1.1	20250710	Updated Resolution information	July 14, 2025
1.2	20250710	Updated Resolution information	July 15, 2025
1.3	20250710	Removed CVE-2025-44954. Updated KSP name for both 6.1.2 and 7.1	July 18, 2025
1.4	20250710	Updated KSP name for 5.2.2	July 21, 2025
1.5	20250710	Updated KSP name for 5.2.1.3	July 23, 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.

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, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, LLC 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.