Security Advisory: ID 20210511

RUCKUS AP Aggregation And Fragmentation Attacks Vulnerability (aka "FragAttacks")

Internal Release Date: **05/11/2021**
Public Release: **05/11/2021**

What is the issue?
The Wi-Fi Alliance publicly disclosed the "Aggregation & Fragmentation Attacks Against Wi-Fi" vulnerabilities on May 11th, 2021.

These vulnerabilities affect the Wi-Fi components of RUCKUS Indoor and Outdoor Access Points, which may allow an adversary to forge encrypted frames, allowing exfiltration of data from the network. Devices using encryption schemes WEP, WPA, WPA2, and WPA3 are all affected.

The following table provides a list of the applicable CVE IDs and a high-level description of each vulnerability:

CVE ID	Description
CVE-2020-24587	Mixed key attack: A vulnerable device reassembles fragments encrypted under different keys in a protected network.
CVE-2020-24588	Frame aggregation attack: Devices allow the encrypted payload to be parsed as containing one or more aggregated frames instead of a normal network packet.
CVE-2020-26139	An Access Point (AP) forwards EAPOL frames to other clients even though the sender has not yet successfully authenticated to the AP. This might be abused in projected Wi-Fi networks to launch denial-of-service attacks against connected clients and makes it easier to exploit other vulnerabilities in connected clients.
CVE-2020-26140	The WEP, WPA, WPA2, and WPA3 implementations accept plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.
CVE-2020-26141	The Wi-Fi implementation does not verify the Message Integrity Check (authenticity) of fragmented TKIP frames. An adversary can abuse this to inject and possibly decrypt packets in WPA or WPA2 networks that support the TKIP data-confidentiality protocol.
CVE-2020-26143	The WEP, WPA, WPA2, and WPA3 implementations accept fragmented plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.
CVE-2020-26144	The WEP, WPA, WPA2, and WPA3 implementations accept plaintext A-MSDU frames as long as the first 8 bytes correspond to a valid EAPOL LLC/SNAP header. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.

CVE ID	Description
CVE-2020-26145	The WEP, WPA, WPA2, and WPA3 implementations accept second (or subsequent) broadcast fragments even when sent in plaintext and process them as full unfragmented frames. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.
CVE-2020-26146	The WPA, WPA2, and WPA3 implementations reassemble fragments with non-consecutive packet numbers. An adversary can abuse this to exfiltrate selected fragments. This vulnerability is exploitable when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used. Note that WEP is vulnerable to this attack by design.
CVE-2020-26147	The WEP, WPA, WPA2, and WPA3 implementations reassemble fragments even though some of them were sent in plaintext. This vulnerability can be abused to inject packets and/or exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used.

Please note that RUCKUS APs are not vulnerable to CVE-2020-24586 and CVE-2020-26142.

What action should I take?

RUCKUS is releasing the fix for these vulnerabilities through a software update. Since these are high severity issues, all affected customers are strongly encouraged to apply the fix as soon as possible.

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

Are there any workarounds available?

There is no workaround that addresses these vulnerabilities, although some mitigation strategies will reduce the risk for successful exploitation of these vulnerabilities. Please read the FAQ page (http://www.commscope.com/fragattacks-commscope-ruckus-resource-center/faqs) for details.

What is the impact on RUCKUS products?

For detailed information concerning vulnerable APs, software versions, target patch release schedules, and recommended actions, please refer to the support page at https://support.ruckuswireless.com/fragattacks-ruckus-technical-support-response-center. Please check this support page periodically as the information is frequently updated.

When will this RUCKUS Security Advisory be publicly posted?

RUCKUS released the initial security advisory to RUCKUS field teams on: 05/11/2021
RUCKUS released the initial security advisory to customers on: 05/11/2021
Public posting: 05/11/2021

Revision History

Version	ID	Change	Date
1.0	20210511	Initial Release	May 11, 2021
1.1	20210511	Added reminder text for checking support portal	Oct 15, 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.

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, 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.