Security Advisory: ID 20211213

CVE-2021-44228: Apache Log4j Vulnerability

Initial Internal Release Date: 12/13/2021
Initial Release to the Public: 12/13/2021
Update Release Date: 12/17/2021
Document Version: 1.3

What is the issue?
A vulnerability was found in the Apache Log4j logging library from version 2.0 to 2.15.0. Products utilizing this library are susceptible to remote code execution vulnerability, where a remote attacker can leverage this vulnerability to gain full control of the impacted device.

For more details about this vulnerability, please see https://nvd.nist.gov/vuln/detail/CVE-2021-44228 and https://nvd.nist.gov/vuln/detail/CVE-2021-45046.

What action should I take?
RUCKUS is releasing the fix for these vulnerability through a software update. Since it is a critical issue, all affected customers are strongly encouraged to apply the fix once available.

For detailed information concerning vulnerable APs, software versions, target patch release schedules, and recommended actions, please refer to the support page at http://support.ruckuswireless.com/log4j-ruckus-technical-support-response-center. Please check this support page periodically as the information is frequently updated.

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?
No.

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
FlexMaster	TBD	TBD	12/23/2021
RUCKUS Analytics	All versions	No action required. Patches will update into production on release date.	12/20/2021
RUCKUS Cloud	21.11	TBD	TBD
SCI	TBD	SCI (Cloud): no action required. Patches will update into production on release date.	• SCI (Cloud) 12/16/2021 • SCI (standalone

		SCI (standalone/on-prem): TBD	/on-prem) TBD
SmartZone and Virtual SmartZone	5.0 to 6.0	KSP patch files published to RUCKUS Support Portal.	• SZ 6.0 KSP 12/17/2021 • SZ 5.2.2 P1 and 5.2.2 KSPs 12/17/2021 • SZ 5.1 and 5.0 KSPs 12/17/2021
SmartZone and Virtual SmartZone FIPs	5.2.1.3 Other SZ FIPS Releases	KSP patch files published to RUCKUS Support Portal. Install KSP when available in Support Portal.	SZ FIPS 5.2.1.3 KSP 12/17/2021 TBD
Unleashed Multi-Site Manager (UMM)	TBD	TBD	12/21/2021

The following products are **not vulnerable**: All Access Points (including Unleashed APs), Cloudpath, ICX Switches, IoT, RUCKUS Network Director (RND, for versions 3.0 and earlier), SmartZone DataPlane, SPoT/vSPoT, Unleashed, and ZoneDirector.

The following products are under assessment: MobileApps, and RUCKUS LTE (CBRS) (including LTE APs).

When will this RUCKUS Security Advisory be publicly posted?
RUCKUS released the initial security advisory to RUCKUS field teams on: 12/13/2021
RUCKUS released the initial security advisory to customers on: 12/13/2021
Public posting: 12/13/2021

Revision History

Version	ID	Change	Date
1.3	20211213	Updated Release	Dec 17, 2021
1.2	20211213	Updated Release	Dec 15, 2021
1.1	20211213	Updated Release	Dec 14, 2021
1.0	20211213	Initial Release	Dec 13, 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.