Ruckus Networks - Security Advisory

ID 20191224 FAQ

ZoneDirector and Unleashed Unauthenticated Remote Code Execution and Other Vulnerabilities – CVE-2019-19834, CVE-2019-19835, CVE- 2019-19836, CVE-2019-19837, CVE-2019-19838, CVE-2019-19839, CVE-2019-19840, CVE-2019-19841, CVE-2019-19842, CVE-2019-19843

Initial Internal Release Date: **12/24/2019**
Initial Release to the Public: **12/24/2019**
Update Release Date: **02/28/2020**

What is the issue?

A number of security vulnerabilities are found on the ZoneDirector and Unleashed product lines. Collectively, these vulnerabilities allow an attacker to perform the following actions:

- Unauthenticated, remote code executions and unauthorized command line interface (CLI) and shell access
- Command injections
- Unauthenticated stack overflow
- Unauthenticated arbitrary file writing
- Server-Side Request Forgery (SSRF)

The following table provides a list of the CVE IDs and a high-level description of their vulnerabilities.

CVE ID	Description
CVE-2019-19834	Command injection vulnerability via a crafted CLI command with admin privilege
CVE-2019-19835	SSRF vulnerability in zap, caused by insufficient input validation
CVE-2019-19836	Remote code execution vulnerability in zap caused by insufficient input validation
CVE-2019-19837	Information disclosure vulnerability
CVE-2019-19838, CVE-2019-19839, CVE-2019-19841, CVE-2019-19842	Remote command injection via a crafted HTTP request, caused by insufficient input validation
CVE-2019-19840	Stack buffer overflow/remote code execution vulnerability via a crafted unauthenticated HTTP request
CVE-2019-19843	Access control vulnerability resulting in sensitive information disclosure

Ruckus Networks would like to recognize and thank Gal Zror of Aleph Research (Security Research by HCL Technologies) for finding and reporting these issues to us.

What action should I take?
Ruckus Networks is releasing the fix for these vulnerabilities through a software update. Because these are CRITICAL issues, all customers are strongly encouraged to apply the fix once available.

Customers with valid support contracts that entitle them to regular updates should download the fix through regular channels. Non contract customers may also obtain the described fixes by contacting Ruckus TAC through regular means as described 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.

What is the impact on Ruckus products?
The following table describes the vulnerable products, software versions, and the recommended actions.

Product	**Vulnerable Release**	**Resolution**	**Patch Release Date**
ZoneDirector	9.9 and before	Upgrade to 9.10.2.0.84 or newer (*)	N/A
	9.10.x	Upgrade to 9.10.2.0.84	Dec 24, 2019
	9.12.x	Upgrade to 9.12.3.0.136	Dec 12, 2019
	9.13.x, 10.0.x	Upgrade to 10.0.1.0.90	Dec 24, 2019
	10.0.x	Upgrade to 10.0.1.0.90	Dec 24, 2019
	10.1.x	Upgrade to 10.1.2.0.275	Oct 25, 2019
	10.2.x	Upgrade to 10.2.1.0.147	Nov 15, 2019
	10.3.x	Upgrade to 10.3.1.0.21	Dec 4, 2019
Unleashed	200.6 and before	Upgrade to 200.7.10.202.94	Dec 24, 2019
	200.7	Upgrade to 200.7.10.202.94	Dec 24, 2019

(*): Some EOL AP are not upgradable. Please contact Customer Support https://support.ruckuswireless.com/contact-us for details.

How does Ruckus qualify severity of security issues?
Ruckus Networks typically utilizes the Common Vulnerability Scoring System (CVSS) v3. This rating system is a vendor-agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response. The following table provides a list of the CVE IDs, their CVSS scores, their vector information.

CVE ID	CVSS 3.0 Base Score	Vector
CVE-2019-19834	7.2	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
CVE-2019-19835	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2019-19836	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-19837	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVE-2019-19838	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-19839	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-19840	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-19841	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-19842	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

When will this Ruckus Security Advisory be publicly posted?

Ruckus Networks released the initial security advisory to Ruckus field teams on: 12/24/2019 Ruckus Networks released the initial security advisory to customers on: 12/24/2019

Public posting: 12/24/2019

Revision History

Version	ID	Change	Date
1.0	20191224	Initial Release	Dec 24, 2019
1.1	20191224	Updated acknowledgement, Support details.	Dec 26, 2019
1.2	20191224	Added non-supported release	Jan 6, 2020
1.3	20191224	Updated CVE information	Feb 28, 2020

Ruckus Support

The Ruckus Networks 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.