Security Advisory: ID 20200615 FAQ

ZoneDirector and Unleashed Unauthenticated Remote Code Execution and Other Vulnerabilities – CVE-2020-13913, CVE-2020-13914, CVE-2020-13915, CVE-2020-13916, CVE-2020-13917, CVE-2020-13918, CVE-2020-13919

Internal Release Date: **06/15/2020**
Public Release: **06/15/2020**

What is the issue?
A number of security vulnerabilities are found on the ZoneDirector and Unleashed product lines. Collectively, these vulnerabilities allow a remote attacker to perform the following actions:

- Reflective XSS via an unauthenticated, crafted HTTP request.
- Denial of Service on web services via unauthenticated, crafted HTTP request.
- Admin credential overwrite via unauthenticated, crafted HTTP request.
- Stack overflow and remote code execution via unauthenticated, crafted HTTP request.
- System information leakage via an unauthenticated, crafted HTTP request.
- Command injection via authenticated, crafted CLI command, and HTTP request.

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

CVE ID	Description
CVE-2020-13913	Reflective XSS via an unauthenticated crafted HTTP request.
CVE-2020-13914	Denial of service attack on AP web service via an unauthenticated crafted HTTP request.
CVE-2020-13915	Admin credential overwrite via an unauthenticated crafted HTTP request (Unleashed only).
CVE-2020-13916	Stack buffer overflow/remote code execution vulnerability via an unauthenticated, crafted HTTP request (Unleashed only)
CVE-2020-13918	System information leakage via an unauthenticated, crafted HTTP request.
CVE-2020-13919	Command injection via an authenticated, crafted HTTP request.

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. Since most of these are CRITICAL issues, all customers are strongly encouraged to apply the fix once available.

For details on the ZoneDirector upgrade process, please see

https://support.ruckuswireless.com/articles/000010079.

In case of any questions contact 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 9.10.2.0.114	May 29, 2020
	9.12.x	Upgrade to 9.12.3.0.154	May 15, 2020
	9.13.x, 10.0.x	Upgrade to 10.0.1.0.123	May 21, 2020
	10.0.x	Upgrade to 10.0.1.0.123	May 21, 2020
	10.1.x	Upgrade to 10.1.2.0.306	May 10, 2020
	10.2.x	Upgrade to 10.2.1.0.183	May 15, 2020
	10.3.x	Upgrade to 10.3.1.0.42	May 26, 2020
	10.4.0	Upgrade to 10.4.0.0.98	May 26, 2020
Unleashed	200.6 and before	Upgrade to 200.7.10.202.118	Jun 1, 2020
	200.7	Upgrade to 200.7.10.202.118	Jun 1, 2020
	200.8	Upgrade to 200.8.10.3.278	May 30, 2020

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

When will this Ruckus Security Advisory be publicly posted?
Ruckus Networks released the initial security advisory to Ruckus field teams on: 06/15/2020
Ruckus Networks released the initial security advisory to customers on: 06/15/2020
Public posting: 06/15/2020

Revision History

Version	ID	Change	Date
1.0	20200615	Initial Release	June 15, 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.