

ID 20190603 FAQ

Ruckus SmartZone Privilege Escalation Vulnerability

Initial Internal Release Date: **06/03/2019**

Initial Release to the public: **06/03/2019**

Update Release Date: **08/12/2019**

This "Ruckus Networks Security Advisory" constitutes Ruckus Networks (an ARRIS company) Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Networks (an ARRIS company).

What is the issue?

Ruckus Network's SmartZone products contain a vulnerability that allows an authenticated attacker to perform privilege escalation action on the affected device through a crafted command via the management interface.

The vulnerability is due to inadequate input validation. A successful exploit could allow the attacker to access files, or even obtain shell access on an affected device.

This vulnerability is first reported by Secfault Security & Security Labs, and then by Aaron Levy from Clover Network, Inc.

What action should I take?

Ruckus Networks is releasing the fix for this vulnerability via software update. Since this is a serious issue, all customers are strongly encouraged to apply this fix to all the relevant devices immediately.

Are there any workarounds available?

To reduce the attack surface, one can consider disabling port 22.

What is the impact on Ruckus products?

All SmartZone software prior to R5.1.1 are vulnerable, except for:

- R3.4.2 Patch-4 and later
- R3.6.2 Patch-2 and later

The following table describes the vulnerable software version and the recommended action:

Product	Vulnerable Release	Resolution	Patch Release Date
Smart-Zone	3.0, 3.1.x, 3.2.x, 3.4.x 3.5.x, 3.6.x 5.0/5.1	Upgrade to 3.4.2 Patch 4 Upgrade to 3.6.2 Patch 2 Upgrade to 5.1.1	May 2019 Oct 2019 May 2019

ID 20190603 FAQ

How does Ruckus qualify severity of security issues?

Ruckus Wireless 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. Below are the CVSS scores and vector information:

CVE ID	CVSS 3.0 Base Score	Vector
CVE-2019-11630	8.0 (HIGH)	(AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

When will this Ruckus Security Advisory be publicly posted?

Ruckus Wireless released the initial security advisory to Ruckus field teams on: 06/03/2019

Ruckus Wireless released the initial security advisory to customers on: 06/03/2019

Public posting: 06/03/2019

Revision History

Version	ID	Change	Date
1.0	20190603	Initial Release	June 3 rd , 2019
1.1	20190603	Minor correction	June 5 th , 2019
1.2	20190603	Corrected info/date concerning 3.6.2	Aug 12 th , 2019

Ruckus Support can be contacted as follows:

The full contact list is at: <https://support.ruckuswireless.com/contact-us>

DISCLAIMER

THIS RUCKUS NETWORKS SECURITY ADVISORY INCLUDING THE INFORMATION IT CONTAINS AND THE PROGRAMS MADE AVAILABLE THROUGH THE LINKS THAT IT INCLUDES, IS PROVIDED TO YOU ON AN "AS IS" BASIS. RUCKUS NETWORKS (AN ARRIS COMPANY) AND ITS SUPPLIERS DO NOT WARRANT THAT SUCH INFORMATION OR THE FUNCTIONS CONTAINED IN SUCH PROGRAMS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PROGRAMS WILL BE UNINTERRUPTED OR ERROR-FREE. THE INFORMATION AND PROGRAMS ARE PROVIDED TO YOU WITH NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT WILL RUCKUS NETWORKS (AN ARRIS COMPANY), ITS SUPPLIERS, OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE INFORMATION OR PROGRAMS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOST DATA, THAT MAY ARISE OUT OF YOUR USE OF OR FAILURE TO USE THE INFORMATION OR PROGRAMS, EVEN IF RUCKUS NETWORKS (AN ARRIS COMPANY) OR SUCH OTHER ENTITIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING SHALL NOT BE DEEMED TO PRECLUDE ANY LIABILITY, WHICH UNDER APPLICABLE PRODUCTS LIABILITY LAW, CANNOT BE PRECLUDED BY CONTRACT.

This "Ruckus Networks Security Advisory" constitutes Ruckus Networks (an ARRIS company) Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Networks (an ARRIS COMPANY).

© Copyright 2019 Ruckus Networks, an Arris company. All Rights Reserved



Ruckus Networks - Security Advisory



ID 20190603 FAQ