Ruckus Networks - Security Advisory
ID 20180516 FAQ

Ruckus SmartZone Sensitive Information Disclosure Vulnerability

Initial Internal Release Date: **05/16/2018**
Initial Release to the public**: *05*/16/2018**
Update Release Date: **05/22/2018**

What is the issue?
Ruckus Network's SmartZone products contain a vulnerability that allows an unauthenticated attacker to retrieve or even tamper sensitive information in the system via a certain network access. This vulnerability is reported by TigerHuang, an independent security researcher.

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?
Currently, no workaround is available. The use of a properly configured firewall is not considered adequate because the system is still vulnerable from attack behind the firewall.

What is the impact on Ruckus products?
Ruckus SmartZone products (vSZ-H, vSZ-E, SZ-100, SZ-300, and SCG-200) running release 3.5.0, 3.5.1, 3.6, and 3.6.1 are impacted.

When will this Ruckus Security Advisory be publicly posted?

Platform	Release*	Target Patch Release Date
SmartZone	3.5.0 3.5.1 3.6.1	May 16th, 2018
SmartZone	3.6.0	May 22nd, 2018

How does Ruckus qualify severity of security issues?
This is a Ruckus SmartZone internal vulnerability and no CVE ID has been issued yet.

When will this Ruckus Security Advisory be publicly posted?

Ruckus Wireless released the initial security advisory to Ruckus field teams on: 05/16/2018
Ruckus Wireless released the initial security advisory to customers on: 05/16/2018
Public posting: 05/16/2018

Revision History

Version	ID	Change	Date
1.0	20180516	Initial Release	May 16, 2018
1.1	20180516	Updated patch release date for 3.6.0, other minor update.	May 22, 2018

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 NONINFRINGEMENT. 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).