

**ID 20181102 FAQ****Libssh Vulnerabilities – CVE-2018-10933**

Initial Internal Release Date: **11/02/2018**

Initial Release to the public: **11/02/2018**

Update Release Date: **11/02/2018**

*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).*

**Summary**

A vulnerability has been published in libssh's server-side state machine which may be exploited by a malicious client to gain unauthorized access.

**What is the issue?**

These vulnerabilities are assigned the CVE IDs and details of the same are explained as below:

<b>CVE ID</b>	<b>CVE Description</b>
CVE-2018-10933	libssh's server-side state machine before versions 0.7.6 and 0.8.4. A malicious client could create channels without first performing authentication, resulting in unauthorized access.

**What is the impact on Ruckus products?**

No Ruckus products are impacted.

**What is the impact on ICX family of switches that are part of Ruckus now?**

No ICX family of switches are impacted.

**Why are Ruckus products not impacted?**

No Ruckus products packages or deploys this module. Hence we are not impacted.

Please refer to some caveats below.

**Caveats:**

Some of Ruckus SZ controller products may have the module packaged, rest assured that they are totally unused. We will be removing the same in future software releases.

**What action do I take?**

No immediate action is required.

**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. In cases where CVSS v3 scores

## ID 20181102 FAQ

are not available, CVSS v2 score are provided. Below are the CVSS scores and vector information for respective CVEs:

CVE ID	CVSS 3.0 Base Score	Vector
CVE-2018-10933	9.1 (Critical)	(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)

### Revision History

Version	ID	Change	Date
1.0	20181102	Initial Release	November 02, 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).

© Copyright 2018 Ruckus Networks, an Arris company. All Rights Reserved