

---

## ID 101717 FAQ

# Multiple Vulnerabilities discovered in RSA key generation within Infineon TPM

Initial Release Date: **10/17/2017**

Document Version: 1.0

*This "Ruckus Security Advisory" constitutes Ruckus (Part of Brocade Inc.) Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus (Part of Brocade Inc).*

### What are the issues?

Ruckus has been made aware of a security weakness in RSA key generation in Infineon-developed TPM firmware.

A summary of the vulnerabilities is disclosed in [CVE-2017-15361](#)

The Infineon RSA library 1.02.013, which is used by Infineon Trusted Platform Module (TPM) firmware (i.e. **SLB 9645 TPM 1.2: FW 133.32**), is reported to suffer a security vulnerability related to RSA key generation. The reported vulnerability makes it easier for attackers to defeat cryptographic protection mechanisms which make use of the affected RSA key. Examples of affected technologies include BitLocker with TPM 1.2.

### What is the impact on Ruckus products?

Ruckus products are not impacted by the reported vulnerability.

Ruckus access points do use Infineon TPM 1.2 (i.e. **SLB 9645 TPM 1.2: FW 133.32**) to store a certificate which is used for product authentication by Ruckus. However, to exploit the Infineon vulnerability, an attacker would require direct access to the TPM component, which is independently protected by Ruckus software. Access to the TPM component is protected by an additional public-private key which is not affected by the Infineon firmware vulnerability.

### Workarounds

No workaround is necessary, since Ruckus products are not compromised by this vulnerability.

As a matter of best practice, Ruckus will update the firmware used by Infineon TPM parts in newly shipping access points as soon as Infineon publishes firmware which fixes the vulnerability. In addition, once available, Ruckus will publish updated TPM firmware as well as instructions on how to perform the upgrade on Ruckus' Support site.

### How does Ruckus Wireless 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

## ID 101717 FAQ

urgency and priority of response. In cases where CVSS v3 scores are not available, CVSS v2 score are provided. Below are the CVSS scores and vector information for respective CVEs:

Note: Since the status of the CVE is under “Awaiting Analysis”, hence there are no NIST based scores officially published for these issues on the date of publishing of this advisory.

CVE ID	CVSS Base Score	Vector
CVE-2017-15361	Not Available	Not Available

### Document Revision History

Version	ID	Change	Date
1.0	101717	Initial Publication	October 17, 2017

### Ruckus Support can be contacted as follows:

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

### STATUS OF THIS NOTICE: Initial release

Although Ruckus Wireless has made all the efforts to make sure that the facts and content stated in this advisory should be best of our ability, however, Ruckus Wireless cannot guarantee the accuracy of all statements in this advisory due to complete publication for the CVE is not done yet. Should there be a significant change in the facts, Ruckus may update this advisory.

### DISCLAIMER

THIS RUCKUS WIRELESS 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 WIRELESS (PART OF BROCADE INC.) 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 WIRELESS (PART OF BROCADE INC.), 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 (PART OF BROCADE INC.) 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 Wireless Security Advisory” constitutes Ruckus Wireless (Part of Brocade Inc.) Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Wireless (Part of Brocade Inc).

© Copyright 2017 Ruckus Wireless (Part of Brocade Inc). All Rights Reserved