
ID 20180116 FAQ

Intel Management Engine impersonation security vulnerabilities

Initial Internal Release Date: **01/16/2018**

Initial Release to the public: **01/16/2018**

Update Release Date: **01/16/2018**

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

This is in response to Intel's recent security advisory released after review of ME/SPS/TXE Intel products. Intel has enumerated the platforms and the firmware versions impacted by these security vulnerabilities. Intel's complete security advisory can be found here: <https://security-center.intel.com/advisory.aspx?intelid=intel-sa-00086&languageid=en-fr>

What are the issues?

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

CVE ID	CVE Description
CVE-2017-5711	Multiple buffer overflows in Active Management Technology (AMT) allow attacker with local access to the system to execute arbitrary code with AMT execution privilege.
CVE-2017-5712	Buffer overflow in Active Management Technology (AMT) allows attacker with remote Admin access to the system to execute arbitrary code with AMT execution privilege.

ID 20180116 FAQ**What is the impact on Ruckus products?**

No Ruckus products are impacted.

Why are Ruckus products not impacted?

Ruckus has reviewed the Intel security advisory and we identified SZ-100 as the only product using the processor hardware and firmware combination that have been marked by Intel as vulnerable. However, since Ruckus does not install the AMT feature drivers into our Operating System, SZ-100 is not impacted. The same has also been confirmed by running vendor-provided tools to verify our results.

What action do I take?

No immediate action is required.

ID 20180116 FAQ**Revision History**

Version	ID	Change	Date
1.0	20180116	Initial Release	January 16, 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