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**

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