

# Intel® Active Management Technology (Intel® AMT) Technical Advisory

Potential Vulnerability of Un-Provisioned Intel® vPro platforms with Intel AMT with a Default Password to Local Provisioning

Originally published September 14 2015

Updated: January 25, 2018

---

## **Products Affected**

Intel® vPro™ platforms and some workstation platforms containing Intel® Active Management Technology

## **Issue Description**

The Bundesamt für Sicherheit in der Informationstechnik (BSI) published the advisory Kurzinfo CB-K15/1256 at <https://www.cert-bund.de/advisoryshort/CB-K15-1256> describing a potential vulnerability of some un-provisioned Intel vPro platforms containing Intel Active Management Technology (Intel AMT) to unauthorized local provisioning using a USB thumb drive.

Separately in 2017, security researchers have raised concerns that Intel AMT can be provisioned by a physical access attack when the *default* Intel® Management Engine BIOS Extension (Intel® MEBX) *password* has not been changed.

## **Intel's Recommendation**

While Intel is not aware of any reported cases of exploitation of the vulnerability described above, Intel is proactively providing the following responses and recommendations:

Intel has made changes to BIOS reference code to (1) clarify terminology used in BIOS Setup programs regarding enabling and disabling of Intel AMT functionality; (2) define expected behavior regarding local provisioning using USB thumb drives; and (3) clarified guidance to systems manufacturers to help protect the Intel MEBX menu with the BIOS password. Intel is working with system manufacturers to help implement the terminology and behavioral changes made in the BIOS reference code.

Intel recommends that IT and security good practices be followed for managing physical access to computer systems and managing passwords, including but not limited to changing of default passwords. The Intel AMT default password can be changed by one of the following methods:

- During the remote provisioning process of Intel AMT computer systems into Admin Control Mode. Refer to the Intel® Setup and Configuration Software (Intel® SCS) User Guide for instructions. [1][2]
- Using a USB thumb drive configured by Intel SCS. Refer to the Intel SCS User Guide for instructions. [1]
- Entering the Intel MEBX locally by pressing a special key combination (usually Ctrl-P) during system POST and following the prompts to change the password. [2]
- Specifying a non-default Intel® MEBX password during manufacture by the system manufacturers. Contact the system manufacturer for availability of this method and specific processes.

## **Acknowledgements**

Bundesamt für Sicherheit in der Informationstechnik (BSI)

## **References**

[1] Intel Corporation. Intel® Setup and Configuration Software (Intel® SCS) User Guide. <http://www.intel.com/go/SCS>.

Accessed 01/25/2018

[2] Intel Corporation. Intel® Active Management Technology (Intel® AMT) Support information.

<https://www.intel.com/content/www/us/en/support/products/23549/technologies/intel-active-management-technology-intel-amt.html>. Accessed 01/25/2018