May 15th, 2017

Advantech Product Security Bulletin
Intel Firmware Vulnerability

Intel® Active Management Technology (AMT), Intel® Small Business Technology (SBT), and Intel® Standard Manageability (ISM) may be vulnerable to remote privilege escalation, which may allow a remote, unauthenticated attacker to execute arbitrary code on the system. The information in this Security Bulletin should be acted upon as soon as possible.

Overview:

There is an escalation of privilege vulnerability in Intel® Active Management Technology (AMT), Intel® Standard Manageability (ISM), and Intel® Small Business Technology (SBT) versions firmware versions 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5, and 11.6 that can allow an unprivileged attacker to gain control of the manageability features provided by these products. This vulnerability does not exist on Intel-based consumer PCs with consumer firmware, Intel servers utilizing Intel® Server Platform Services (Intel® SPS), or Intel® Xeon® Processor E3 and Intel® Xeon® Processor E5 workstations utilizing Intel® SPS firmware.

References:

1. Intel Security Advisory (INTEL-SA-00075): https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr
2. White-papers (Maksim Malyutin from Embedi who highlight this issue) https://www.embedi.com/files/white-papers/Silent-Bob-is-Silent.pdf
3. Intel News: https://newsroom.intel.com/news/important-security-information-intel-manageability-firmware/
4. US-CERT: https://www.us-cert.gov/ncas/current-activity/2017/05/01/Intel-Firmware-Vulnerability
5. JPCERT: http://jvn.jp/vu/JVNVU92793783/
6. Taiwan CERT: https://www.twcert.org.tw/twcert/advdetail/3382

Advantech Headquarters | No. 1, Alley 20, Lane 26, Rueiguang Road, Neihu District, Taipei 11491, Taiwan, R.O.C. | ☎ +886-2-2792-7818|🖷 +886-2-2794-7301

Description:

Intel offers a number of hardware-based remote management technologies meant for maintenance of computer systems. These technologies include Intel® Active Management Technology (AMT), Intel® Small Business Technology (SBT), and Intel® Standard Manageability (ISM), and the Intel Management Engine. That including platform Arrandale/Nehalem, Sandy Bridge, Ivy Bridge, Haswell, Broadwell, Skylake and Kaby Lake.

These technologies listen for remote commands on several known ports. Intel's documentation provides that ports 16992 and 16993 allow web GUI interaction with AMT. Other ports that may be used by AMT include 16994 and 16995, and 623 and 664.

The Intel Management Engine that supports these technologies is vulnerable to a privilege escalation that allows an unauthenticated attacker to gain access to the remote management features provided by the Intel Management Engine. Intel has released a security advisory as well as a mitigation guide with more details.

Impact:

A remote, unauthenticated attacker may be able to gain access to the remote management features of the system. The execution occurs at a hardware system level regardless of operating system environment and configuration.

Recommendation:

Intel has released a downloadable discovery tool located at Intel's download center (https://downloadcenter.intel.com/download/26755), which will analyze your system for the vulnerability. IT professionals who are familiar with the configuration of their systems and networks can use this tool or can find more details below.

- Step 1: (How to identify the product having these potential risks?)
  Determine if you have an Intel® AMT, Intel® SBA, or Intel® ISM capable system by those method of website https://communities.intel.com/docs/DOC-5693. If you determine that you do not have an Intel® AMT, Intel® SBA, or Intel® ISM capable system then no further action is required.

Advantech Headquarters | No. 1, Alley 20, Lane 26, Rueiguang Road, Neihu District, Taipei 11491, Taiwan, R.O.C. | ☎ +886-2-2792-7818|🖷 +886-2-2794-7301

- Step 2: (How to make sure if the BIOS/ME code of product has been upgraded or not?)
  Utilize the Detection Guide to assess if your system has the impacted firmware by download detection tools from Intel's download center. https://downloadcenter.intel.com/download/26755. If you do have a version in the "Resolved Firmware" column no further action is required to secure your system from this vulnerability.

- Step 3: (How to protect your system if the ME/BIOS code was not available to upgrade.)
  If you do not have any plan to use those remote management technologies in the future, simply follow Intel's Mitigation Guide (https://downloadcenter.intel.com/download/26754) to disable OR delete those functions.
  If you do have a plan to use those remote management technologies in the future, please kindly inform Advantech's sales, and we will release a new ME/BIOS code for you soon. However, we still suggest referring to this advisory to identify fixes as they are posted for your systems.
  Options for mitigation until the firmware update is available are:
  - The network vulnerability can be mitigated by unprovisioning the Intel manageability SKU (AMT & ISM) or disabling the Intel manageability technology within the Intel® MEBx.
  - The local vulnerability can be mitigated by disabling or uninstalling Local Manageability Service (LMS) on Intel manageability SKUs (AMT, ISM, and SBT).

  Note that capabilities and features provided by AMT, ISM and SBT will be unavailable when these mitigations are implemented. The instructions to implement the mitigation steps are posted on Intel's website (https://downloadcenter.intel.com/download/26754)

Thank you for choosing Advantech products, and we appreciate you are Advantech's valuable customer.

Sincerely,

Advantech
Corporate Quality

Advantech Headquarters | No. 1, Alley 20, Lane 26, Rueiguang Road, Neihu District, Taipei 11491, Taiwan, R.O.C. | ☎ +886-2-2792-7818|🖷 +886-2-2794-7301