CERT-EU Security Advisory 2017-010

Critical Privileges Escalation Vulnerability in Intel AMT Service

May 4, 2017 — v1.1

History:

- *02/05/2017 — v1.0: Initial publication*
- *04/05/2017 — v1.1: Title and wording corrected based on comments from Intel*

Summary

On 1st of May 2017, Intel reported that there is *an escalation of privilege vulnerability in Intel® Active Management Technology (AMT), Intel® Standard Manageability (ISM), and Intel® Small Business Technology 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* [1].

Essentially any PC with vPro and AMT features enabled are at risk, although Intel states in their advisory that *Intel-based consumer PCs* are not affected.

Technical Details

The vulnerability received a CVE label CVE-2017-5689 [2].

According some researchers [3] the problem is so important because affects the AMT service. This service is reachable through the network and has DMA access (direct memory access bypassing the processor) to the system. Which means that after exploiting the vulnerability, the attacker can arbitrarily read and write to memory on the system.

The vulnerable AMT service is part of Intel's vPro suite of processor features. If vPro is present and enabled on a system and AMT is provisioned, unauthenticated users of the local network can access the computer's AMT controls and hijack them, with the above explained consequences. If AMT is not provisioned, a logged-in user can still potentially exploit the bug to gain admin-level powers. If the vPro or AMT is not present at all, the machine is not vulnerable [4].

According to Intel, there are two ways this vulnerability may be exploited (note that Intel® Small Business Technology is not vulnerable to the first issue) [1]:

1. An unprivileged network attacker could gain system privileges to provisioned Intel manageability SKUs: Intel® Active Management Technology (AMT) and Intel® Standard Manageability (ISM).

   `CVSSv3 9.8 Critical /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`

2. An unprivileged local attacker could provision manageability features gaining unprivileged network or local system privileges on Intel manageability SKUs: Intel® Active Management Technology (AMT), Intel® Standard Manageability (ISM), and Intel® Small Business Technology (SBT).

   `CVSSv3 8.4 High /AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`

Products Affected

Impacted: Products with Intel manageability firmware versions 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5, and 11.6 for Intel® Active Management Technology, Intel® Small Business Technology, and Intel® Standard Manageability.

Not impacted: Products with firmware versions before 6 or after 11.6 are not impacted.

Essentially, **every Intel platform with AMT, ISM, and SBT** from **Nehalem** in **2008** to **Kaby Lake** in **2017** has a remotely exploitable security hole [3].

Recommendations

Follow the detection and mitigation procedure described in the *Recommendations* section of the original Intel advisory [1]. As indicated, a patch to the firmware is needed to fix the problem. If applying a patch is not an option, there is a mitigation guide published by Intel [5].

References

[1] Intel security center https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr

[2] CVE https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5689

[3] SemiAccurate article https://semiaccurate.com/2017/05/01/remote-security-exploit-2008-intel-platforms/

[4] The Register article https://www.theregister.co.uk/2017/05/01/intel_amt_me_vulnerability/

[5] Intel mitigation guide https://downloadmirror.intel.com/26754/eng/INTEL-SA-00075%20Mitigation%20Guide-Rev%201.1.pdf