WHITE PAPER

INTEL-SA-00075 Mitigation Guide

Intel® Active Management Technology (Intel® AMT), Intel® Standard Manageability (ISM), and Intel® Small Business Technology (SBT).

Mitigations for security vulnerability documented in INTEL-SA-00075

Revision 1.1 – May 1, 2017

Table of Contents

Executive Summary

This documentation will provide instructions on how to implement mitigations on Intel manageability SKU systems that are vulnerable to a known privilege escalation issue. For more information, please read the Public Security Advisory at https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr.

These mitigations are intended to prevent unauthorized activation and use of Intel manageability SKUs, Intel® Active Management Technology (Intel® AMT), Intel® Standard Manageability (ISM), and Intel® Small Business Technology (SBT) that have not applied the firmware update addressing the vulnerability.

IT practitioners can use these instructions as basis for scripts or tasks within management consoles for scale deployments of the mitigation steps. The procedural steps for implementing the mitigation are as follows:

1. Unprovisioning Intel manageability SKU clients to mitigate unprivileged network attacker from gaining system privileges
2. Disabling or removing the Local Manageability Service (LMS) to mitigate unprivileged local attacker from gaining system privileges
3. Optionally configuring local manageability configuration restrictions

Intel highly recommends that the first step in all mitigation paths is to unprovision the Intel manageability SKU to address the network privilege escalation vulnerability. For provisioned systems, unprovisioning must be performed prior to disabling or removing the LMS. Pending availability of the updated Intel manageability SKU firmware, Intel highly recommends mitigation of the local privilege escalation by removing or disabling the LMS. Optionally, as a second layer of defense against inadvertent reinstall or re-enabling of the LMS, some of the manageability configuration options performed through the OS can additionally be disabled through the operating system (OS); however, these additional local manageability configuration restrictions have constraints on how they are allowed to be reversed.

For assistance in implementing the mitigation steps provided in this document, please contact Intel Customer Support; from the Technologies section, select Intel® Active Management Technology (Intel® AMT).

Step 1: Unprovisioning clients

When configured, Intel® AMT and ISM automatically listen for management traffic over your computer network. Systems that are vulnerable to the known privilege escalation issue should be unprovisioned using the tools used to initially configure them to prevent unauthorized access to manageability features. As an example, the Intel® AMT Configuration Utility (ACUConfig) from the Intel® Setup and Configuration Software (Intel® SCS) download can be used from a command line to unconfigure systems.

Example unconfigure commands (note these will need to be executed with OS administrative rights):

Unconfiguring a system in CCM:

```
ACUConfig.exe UnConfigure
```

Unconfiguring a system in ACM without RCS integration:

```
ACUConfig.exe UnConfigure /AdminPassword
<password> /Full
```

Unconfiguring a system with RCS integration:

```
ACUConfig.exe UnConfigure /RCSaddress
<RCSaddress> /Full
```

See section 6.14, Unconfiguring Intel AMT systems, of the Intel® SCS user guide for additional details. You can download a copy of Intel® SCS and ACUConfig at the following URL: http://www.intel.com/go/scs

Step 2: Disable or remove LMS

Note: Unprovisioning clients and restricting Intel manageability SKU configuration options through the OS have a dependency on LMS running. Perform these steps prior to the disabling or uninstalling LMS.

What is LMS

Intel® Management and Security Application Local Management Service (LMS) is a service that enables local applications running on Intel® AMT, Intel® SBA or Intel® Standard Manageability supported devices to use common SOAP and WS-Management functionality. It listens to the Intel® Manageability Engine (ME) ports (16992, 16993, 16994, 16995, 623, and 664) and routes the traffic to the firmware through the Intel® MEI driver.

Process to disable LMS

Note: The following commands utilize the Windows built in command line program SC for communicating with the Service Control Manager and services. An Active Directory Group Policy Object (GPO) can also be leveraged to scale disabling LMS.

Run the following command from a command prompt with administrative rights:

```
sc config LMS start=disabled
```

Process to remove LMS

Run the following command from a command prompt with administrative rights:

```
sc delete LMS
```

Note: This command removes LMS from Windows services. To fully remove LMS from the system, you need to also delete the executable `LMS.exe`. If you are not sure what the path is, you can find it using the following command from a command prompt:

```
sc qc LMS
```

Additional Considerations

Anyone with OS administrative privileges will be able to reinstall the LMS if it is removed, or re-enable the service if it is disabled. Note that this is not a weakness in the mitigation, because anyone with OS administrative privilege would already have the capabilities that are exposed by the vulnerability. The implication is that it is important to be cautious to avoid an inadvertent re-install or re-enable of the LMS while the vulnerability exist on the system. For example, the LMS could be reinstalled if you ran the Intel manageability software installer sometime in the future.

What are alternate LMS

Management console agents may include an alternative Local Management Service (LMS) to manage Intel manageability SKUs. One examples is MicroLMS, a component of the MeshCentral open source project.

Confirming if a Local Management service is active.

You can confirm the Local Management Service (LMS) and variants of it like MicroLMS are properly disabled by confirming there is no socket listening on the Intel® ME Internet Assigned Names Authority (IANA) ports on the client: 16992, 16993, 16994, 16995, 623, and 664.

This Windows command will show if there is an application listening on the Intel® ME IANA ports:

```
netstat -na | findstr "\<16993\> \<16992\>
\<16994\> \<16995\> \<623\> \<664\>"
```

Note: Although these are the standard ports for LMS, a custom developed LMS could be designed to listen on alternative ports.

Optional Step: Configuring local manageability configuration restrictions

Note: The configuration restrictions outlined in this section are optional steps for customers that require a secondary layer to protect against mitigation reversal by an unprivileged attacker who gains OS admin privileges. Reversal of these options are difficult, may not be supported by the computer's manufacturer, and may require physical access to the system. If you choose to perform this additional configuration restriction, it must be performed prior to disabling the LMS service

Steps to disable CCM with ACUConfig

You can disable Client Control Mode (CCM) using ACUConfig, a component of the Intel® Setup and Configuration Software (Intel® SCS). You can obtain a copy of Intel® SCS at the following URL:

http://www.intel.com/go/scs

You can disable CCM using the following command from a command prompt with administrative rights:

```
ACUConfig.exe DisableClientControlMode
```

The suppression of the confirmation prompt can be performed by using the /confirmDisableCCM" command line switch. See section 6.16, Disabling Client Control Mode, of the Intel® SCS user guide for additional details.

Steps to re-enable CCM

If supported by your manufacturer, you may be able to reset Intel manageability SKUs from BIOS, which would re-enable CCM. Consult your manufacturer to see if this capability is supported and for the steps to follow.

Note: Your manufacturer may provide tools that allow you to configure BIOS settings through the OS. These tools, if available, may allow you to reset Intel manageability SKUs in BIOS without having to physically touch the computer. Check with your manufacturer to see if they provide a tool with this functionality.

Steps to disable EHBC with ACUConfig

If your platform supports Embedded Host Based Configuration (EHBC) you can disable it using ACUConfig. This is a permanent change that cannot be reversed without the support of the computer's manufacturer.

You can disable EHBC using the following command from a command prompt with administrative rights:

```
ACUConfig.exe DisableEmbeddedHBC
```

See section 6.18, Disabling the EHBC Option, of the Intel® SCS user guide for additional details.