WHITE PAPER

INTEL-SA-00075 Firmware Deployment Procedure Guidance

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

Firmware deployment procedure guidance for security vulnerability documented in INTEL-SA-00075

Revision 1.0 – May 11, 2017

Table of Contents

Executive Summary

Certain Intel manageability SKU systems are vulnerable to a known privilege escalation issue. Mitigation includes installation of updated system firmware. This document provides the recommended steps for deploying updated firmware to these systems. Read the Intel Public Security Advisory at https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr for more information.

The procedural steps for implementing the mitigation are as follows:

1. Unprovision the Intel manageability SKU system. This is necessary to mitigate the network privilege escalation vulnerability and remove any configuration changes an unprivileged attacker could have made prior to mitigation.
2. Update the impacted systems with firmware obtained from your OEM that addresses this issue.
3. Re-provision Intel manageability SKU with your existing manageability / configuration console.

For large scale deployment of the firmware update and mitigation steps, IT practitioners can use these instructions as the basis for scripts or tasks within management consoles. For assistance in implementing the firmware deployment steps provided in this document, please contact Intel Customer Support; from the Technologies section, select Intel® Active Management Technology (Intel® AMT).

Step 1: Unprovisioning Systems

An unprivileged attacker could have changed the Intel manageability SKU configuration settings, including changing manageability administrative passwords, adding manageability users, and modifying manageability feature settings.

Unprovisioning is not typically required or recommended as part of performing an Intel manageability SKU firmware update. However, to ensure confidence in the Intel manageability SKU configuration settings after discovery of this privilege escalation issue, it is highly recommended that customers perform an unprovision prior to deploying the computer manufacturer's firmware update.

Although performing the unprovision can technically be done after the firmware update, there are more tool options if the unprovisioning is performed prior to deploying firmware that resolves the privilege escalation issue described in the INTEL-SA-00075 Public Security Advisory.

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

Alternative "Unprovisioning Tool":

If the above steps using ACUConfig are unsuitable or unavailable to you, an alternative exists, the "INTEL-SA-00075 Unprovisioning Tool".

You can download a copy of the Unprovisioning tool at the following URL: https://downloadcenter.intel.com/download/26781

After unprovisioning the system, proceed to the required Step 2 below to update firmware.

Step 2: Update Firmware

To ensure that you are obtaining and deploying the correct firmware update for your impacted platform, it will be necessary to work with your computer manufacturer. It is recommended you visit the computer manufacturer's support website to download the latest firmware update for the impacted platforms.

Note: Some manufacturers offer system specific firmware downloads, even within product models. Confirm with your OEM that you have the correct firmware download for each system that requires updating.

Once the firmware update is obtained from the computer manufacturer, follow the OEM's installation instructions and use the tools provided by your OEM to install the firmware update for each affected system.

Step 3: Provision Systems

Once the firmware update is completed, the Intel manageability SKU can be re-provisioned with the existing manageability infrastructure to re-activate the manageability capabilities on the platform.

For details on how to provision the Intel manageability SKU, please visit: http://www.intel.com/content/www/us/en/software/scs-deployment-guide.html