

**How do we detect if we are vulnerable to this threat? What are our mitigation options?**

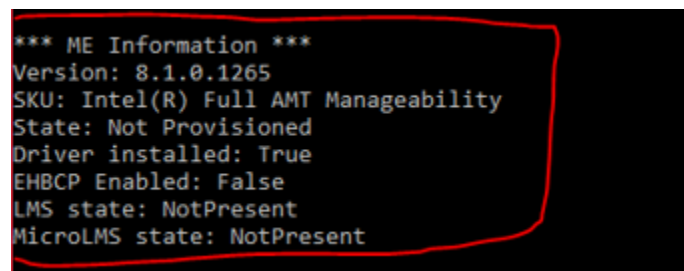
Intel has released a security advisor (INTEL-SA-00075) that affects Dell business PCs that support system manageability via Intel Active management Technology (AMT), Intel Small Business Technology (SBT), or Intel Standard Manageability (ISM).

**BIOS Release Details**

The following list ([here](#)) contains all the possible affected products from DELL *but only those purchased with Intel AMT, SBT, or ISM capability are vulnerable*.

**Determine if machine is vulnerable**

To detect if a machine is vulnerable you have two options to run Intel's (Intel-SA-00075-console.exe) via command prompt or (Intel-SA-00075-GUI.exe). They will both be checking for the *State status*. In this case, this machine is *Not Provisioned* meaning there's smaller chance of it being vulnerable but does not exclude it from vulnerability.



```
*** ME Information ***
Version: 8.1.0.1265
SKU: Intel(R) Full AMT Manageability
State: Not Provisioned
Driver installed: True
EHBCP Enabled: False
LMS state: NotPresent
MicroLMS state: NotPresent
```

**Mitigation Options**

The main mitigation option is to un-provision clients this can be done by un-configuring a system in CCM and ACM. An example provided by Intel's Intel-SA-00075 Mitigation guide

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

Un-configuring a system in CCM:

- ACUConfig.exe UnConfigure

Un-configuring a system in ACM without RCS integration:

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

Un-configuring a system with RCS integration:

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

The next step after this is done is to disable or move LMS(Local Manageability Service). You have two options in this case to disable LMS or to completely remove LMS that can be done with the follow commands

#### **Disable LMS**

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

- **sc config LMS start=disabled**

#### **Remove LMS**

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

- **sc delete LMS**

An alternative is using the “Un-provisioning tool” can be found ([here](#)) the tool is intended to be run on systems where AMT is provisioned and the Local Manageability Service (LMS) is running.