INTEL-SA-00075 Linux* Discovery Tool

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

Instructions for detecting INTEL-SA-00075

Revision 1.25 – May 19, 2017

Summary

This document will step you through the processes to detect INTEL-SA-00075. Read the Public Security Advisory at https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr for more information.

If you are a user of a single Linux* system or a network administrator wishing to determine the status of multiple machines: We provide the INTEL-SA-00075-Discovery-Tool for local analysis of a single or multiple systems.

System Requirements

- Ubuntu* 16.04 LTS or Ubuntu* 14.04 LTS
- The Intel® Management Engine Components, specifically:
    - The Intel® Management Engine Interface driver (Intel® MEI)

Note: The tool does not support Virtual Machine (VM) environment. As a workaround, use LiveCD.

Using the INTEL-SA-00075-Discovery-Tool

What is the INTEL-SA-00075-Discovery-Tool?

The INTEL-SA-00075-Discovery-Tool can be used by local users or an IT administrator to determine whether a system is vulnerable to the exploit documented in Intel Security Advisory INTEL-SA-00075 for systems running Linux* operating system. This is a command line tool.

Meaning of the Vulnerability Status in the console output

The following logic is used to determine the vulnerability status in the output of the screen:

- Not Vulnerable: The system meets the "Not Vulnerable" criteria described in the *Identifying vulnerable systems using the INTEL-SA-00075 Discovery Tool* section of the document.
- Vulnerable: The system has a vulnerable manageability firmware version, firmware needs to be updated. Contact your OEM to receive resolved firmware update.
- Vulnerable, run the unprovision tool: The system has a vulnerable manageability firmware version and is provisioned with Intel® AMT, Intel ISM, or Intel® SBT. The system must be unprovisioned and the firmware needs to be updated. If firmware update is not available, then unprovisioning the system will help to mitigate. If the system was provisioned prior to the firmware update, an attacker using the known vulnerability may have changed the manageability configuration. There is a limited amount of verification that can be done through reviewing the Intel manageability SKU audit log. A full unprovision, reprovision of the manageability SKU will remove unauthorized configuration settings. Additionally, contact your OEM to receive resolved firmware update.

Running the console tool

Download the INTEL-SA-00075-Discovery-Tool binary on the system where vulnerability is to be detected.
Open terminal application and execute the binary using root privileges

e.g. sudo ./INTEL-SA-00075-Discovery-Tool

Note 1:
The Intel® MEI driver exposes a misc device called /dev/mei. An application maintains communication with an Intel® ME feature while /dev/mei is open. By default, the INTEL-SA-00075-Discovery-Tool uses /dev/mei0 node. Ensure that this node is available else the application will result in an error message.
Open Terminal and list available devices

ls /dev/mei*

If the result is a mei* device node where * # 0; then re-run the application with correct node

e.g. sudo ./ INTEL-SA-00075-Discovery-Tool –d /dev/mei#

Figure 1 Example of INTEL-SA-00075-Discovery-Tool Console output

```
INTEL-SA-00075-Discovery-Tool -- Release 0.5
Copyright (C) 2003-2012, 2017 Intel Corporation.  All rights reserved


------------------Firmware Information--------------------

Intel(R) AMT: ENABLED
Flash:  11.0.12
Netstack:       11.0.12
AMTApps:        11.0.12
AMT:    11.0.12
Sku:    16392
VendorID:       8086
Build Number:   1003
Recovery Version:       11.0.12
Recovery Build Num:     1003
Legacy Mode:    False

-----------------SKU Information-----------------
                 Corporate SKU
                 Intel(R) Active Management Technology
-------------------------------------------------

PROVISIONING_STATE = POST
Control Mode: ADMIN / ACM

------------------Vulnerability Status--------------------
Based on the version of the Intel(R) MEI, the System is Vulnerable.
Run the unprovision tool to reset AMT to factory settings.
If Vulnerable, contact your OEM for support and remediation of this system.
For more information, refer to CVE-2017-5689 at:
https://nvd.nist.gov/vuln/detail/CVE-2017-5689 or the Intel security advisory
Intel-SA-00075 at:
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr
-------------------------------------------------------------
```

Table 1 INTEL-SA-00075-Discovery-Tool Console output values

Value	Description	Category
Intel AMT	The firmware SKU is manageability capable	Firmware Information
Flash	Intel® ME Kernel Code Version	
Netstack		
AMTApps		
AMT	Intel® AMT version	
SKU	For Intel® AMT 2.0, Intel® AMT 2.1 and Intel® AMT 2.2 - X - where X is a value of: 0 = AMT + ASF + iQST SKU 1 = ASF + iQST SKU 2 = iQST SKU	SKU Information

	For Intel® AMT Release 2.5 or later releases, this value is a bit combination: 0x00000001 – Reserved 0x00000002 – Intel® Quiet System Technology (From Release 7.0, Reserved) 0x00000004 – ASF (From Release 6.0, Reserved) 0x00000008 – Intel® Active Management Technology From Intel® AMT Release 5.0 or later releases the following options were added: 0x00000010 – Intel® Standard Manageability 0x00000020 – Reserved 0x00000040 – Reserved 0x00000080 – Reserved 0x00000100 – Intel® Remote PC Assist Technology 0x00000200 – 0x00001000– Reserved 0x00002000 – Intel® Anti-Theft Technology - PC Protection 0x00004000 – Corporate (From Release 6.0, KVM supported) 0x00010000 – 0x80000000 – Reserved From Intel® AMT Release 8.0 or later releases, the following options were added: 0x00010000 – Intel® Small Business Technology 0x00020000 – 0x80000000 – Reserved	
Vendor ID	Identifier of Vendor ID. For example: “8086” = Intel Corp. “04b3” = IBM Corp. Reported in Intel® AMT Release 2.0 or later releases.	Firmware Information
Build Number	XXXX Where X is a decimal digit. Describes the build number of the current build: Reported in Intel® AMT Release 2.0 or later releases.	Firmware Information
Recovery Version	XX.YY.ZZZZ Where X, Y, Z are decimal digits.	Firmware Information

	Describes the version of the recovery partition. The reported version might also be "unknown" if recovery partition update fails. Reported in Intel® AMT Release 2.0 or later releases.	
Recovery Build Num	XXXX Where X is a decimal digit. Describes the build number of the recovery partition. The reported number might also be "unknown" if recovery partition update fails. Reported in Intel® AMT Release 2.0 or later releases.	Firmware Information
Legacy Node	"True" or "False" Indicates whether Intel® AMT Release 2.0 (or later) is operating in Intel AMT Release 1.0 Legacy mode. For more information, refer to Section 10.3 Reported in Intel® AMT Release 2.0 or later releases.	Firmware Information
PROVISIONING_STATE	Pre – Un-provisioned system In – Provisioning In-progress Post – Provisioned	

Identifying impacted systems using the INTEL-SA-00075-Discovery-Tool

Impacted systems are defined as having an affected Intel® Management Engine (Intel® ME) firmware version and containing one of three manageability feature sets as defined in the table below.

Table 2 Criteria to determine if a system is vulnerable to INTEL-SA-00075

Value Name	Vulnerable	Not Vulnerable
Intel® ME SKU	Intel® Full AMT Manageability Intel® Standard Manageability Intel® Small Business Advantage(Intel® SBA)	Intel® ME SKU values not present in the vulnerable list to the left -or- Intel® ME SKU values to the left with a firmware version that is not vulnerable
Intel® ME Version	Intel® ME Versions 6.x.x.x – 11.6.x.x with a build value less than 3000 Example: 9.5.22.1760	Intel® ME Versions: • 6.x.x.x – 11.6.x.x with a build value greater or equal to 3000 ○ Example: 11.6.27.3264 • 2.x.x.x. – 5.x.x.x • 11.7.x.x or greater

Note: Intel® Small Business Technology (Intel® SBT) is the manageability SKU for Intel® Small Business Advantage (Intel® SBA)

Troubleshooting

If the tool encountered errors you may see the following error messages on the console output

Result	Explanation
Cannot establish handle to the Intel® MEI driver	Intel® MEI driver is not installed. Contact OEM for further assistance.
Failed connection to Intel® ME Subsystem. Contact OEM	Incorrect Intel® MEI device node. Perform steps in page 2, Note 1. If the steps do not help, there is an error encountered communicating to Intel® ME subsystem. Contact OEM.
Failed to retrieve response for provisioning status	The provisioning status of the system cannot be determined. The application was able to retrieve other firmware information. If your system is vulnerable and provisioning state is not known, contact OEM.