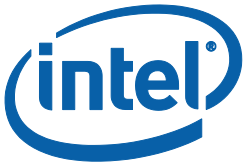

Intel-SA-00125 Detection Tool

User Guide

August 2018

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document. Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit www.intel.com/design/literature.htm.

Intel, and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.
*Other names and brands may be claimed as the property of others.

© 2018 Intel Corporation. All rights reserved

Contents

Table of Figures

1 Introduction

This document will guide you through multiple processes to detect the security vulnerability described in Intel-SA00125. Read the Public Security Advisory at *https://www.intel.com/content/www/us/en/support/articles/000028795.html* for more information.
The following table lists the CVE entries for different versions of firmware. For more information, use the Search function at *https://nvd.nist.gov/vuln/search*.

Intel® Manageability Engine Firmware 11.0/11.5/11.6/11.7/11.10/11.20	CVE-2018-3655

Figure 1: Intel-SA-00125 CVE Entries

If you are a user of a single Windows* PC and you wish to determine its status:
We have provided the **Intel-SA-00125 Detection GUI** application (*Intel-SA-00125-gui.exe*) for local analysis of a single or standalone Windows* system.

If you want to determine the status for multiple Windows* machines:
We have provided the **Intel-SA-00125 Detection Tool Console** application (*Intel-SA-00125-console.exe*). This tool can perform detection and write its findings to the local Windows* Registry, and (optionally) to an XML and/or .txt file, for subsequent collection and analysis.

If you are a user of a Linux* system and you wish to determine its status:
We have provided the **Intel-SA-00125 Detection Console** application (*intel_sa00125*) for analysis of Linux* systems.

Note: The Detection Tool does not support MacOS.

2 Using the Intel–SA–00125 Detection Tool

What is the Intel-SA-00125 Detection Tool?

The Intel-SA-00125 Detection 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-00125*.

The Detection Tool is offered in two versions for Windows* and in a single version for Linux*.

- For Windows* there is an interactive GUI tool that retrieves the device's hardware and software details and provides an indication of risk assessment. This version is recommended for evaluating a local Windows* system.
- The second version, for Linux* and Windows*, is a console executable that can perform the risk assessment and optionally save the detection information to the Windows* registry (Windows* only), to an XML file, and/or to a text file. This version is more convenient for IT administrators who need to perform bulk detection operations across multiple machines.

2.1 Obtaining the Intel-SA-00125 Detection Tool

The Intel-SA-00125 Detection Tool download package is available at https://www.intel.com/content/www/us/en/support/articles/000028795.html .

2.2 System Requirements

Windows*:

- Microsoft* Windows* 7, 8, 8.1, 10 (including 10 S), or 2012 R2 for servers (x64) (Windows*10 IOT Core is not supported)
- .Net version 4.5 or later
- Intel® Management Engine Interface (Intel® MEI) driver
- Administration privileges

Linux*:

- Ubuntu* LTS 16.04 (for client), Redhat 7.2 (for Server)
- Python* 2.6.6
- Local operating system administrative access

2.3 Installing the Tool – Linux*

Unzip the package into a directory.

Ensure that Execute permission is set on the following files:

- intel_sa00125

2.4 Running the Linux* Console Tool

From the installation directory, if Python 2.x is installed, execute the command:
sudo ./intel_sa00125

Note: If Python 3.x (and not Python 2.x) is installed, execute the command:
sudo python3 intel_sa00125

Note: The Linux* tool accepts no command line options.

2.5 Installing the Tool – Windows*

Unzip the downloaded package into a directory.

The console tool can be found in the DiscoveryTool subdirectory. The GUI tool can be found in the DiscoveryTool.GUI directory.

2.6 Running the GUI Tool

Intel-SA-00125-GUI.exe is designed to run on a single system. The tool outputs the detection information to the screen.

Following is an example of the program's output when run on a vulnerable system:

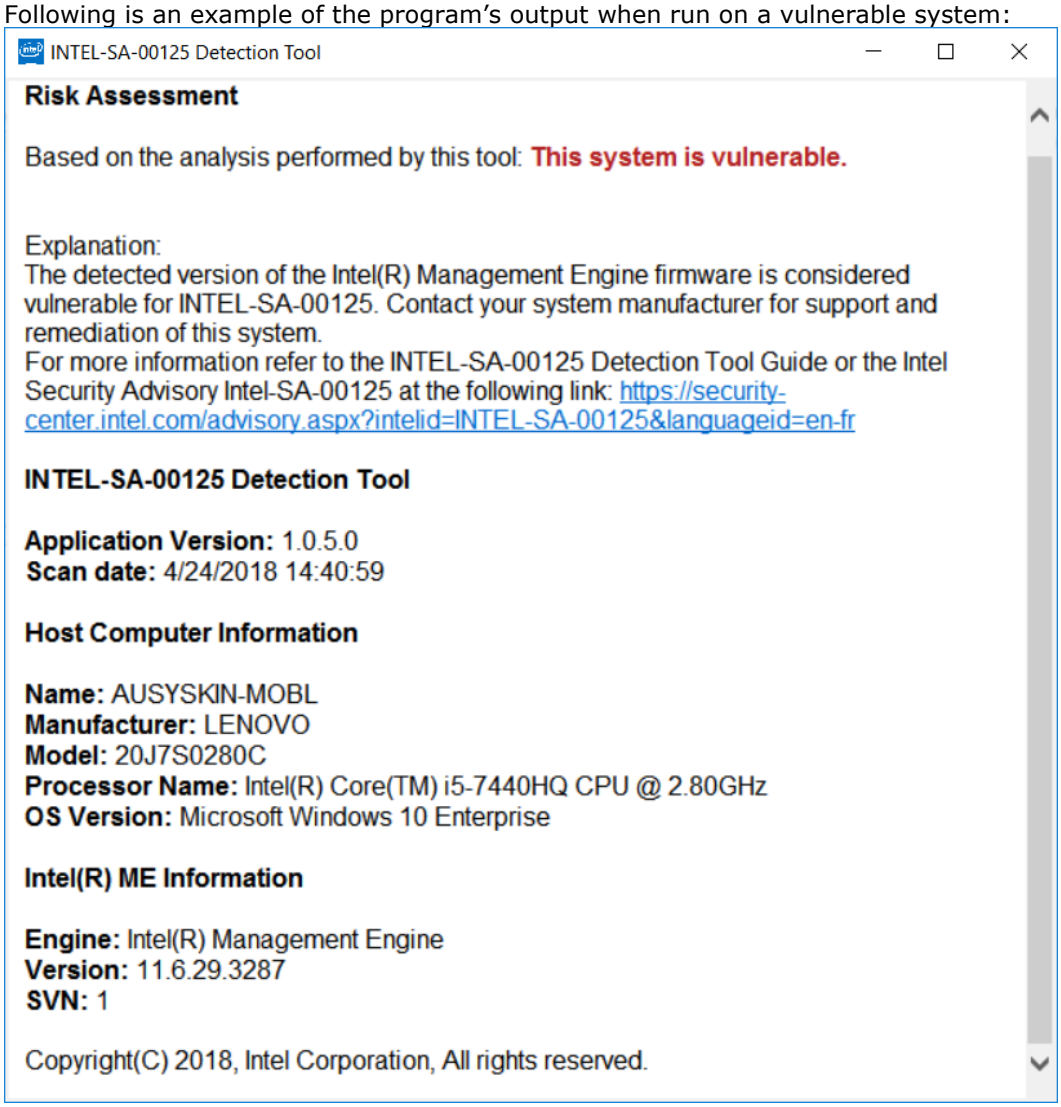

Figure 2: Program Screen Output Example for Vulnerable System

Following is an example of the program's output when run on a system that is not vulnerable:

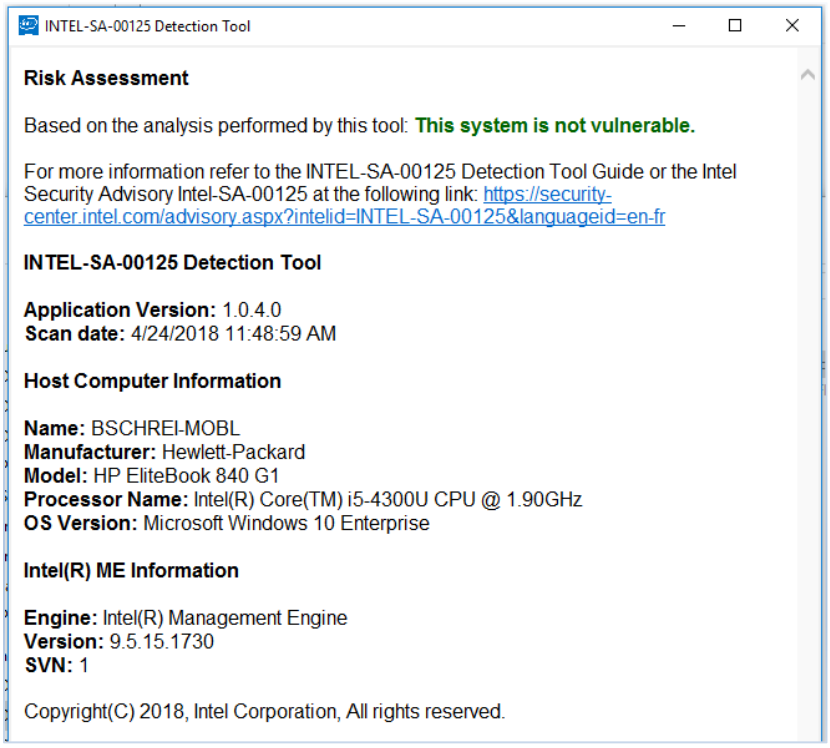

Figure 3: Output Example for System that is Not Vulnerable

Note: *On SPS platforms, the recovery version is displayed in the Intel® ME Information section.

2.7 Running the Windows* Console Tool

Execute **INTEL-SA-00125-console.exe** from a command prompt.

Syntax: Intel-SA-00125-console.exe [[option...]]

The following table shows the program's available options:

Command Line Option	Functionality
-n, --noregistry	Prevents writing results to the registry
-c, --noconsole	Prevents results from being displayed on the console
-p <filepath>, --filepath <filepath>	Path to the directory in which to store the output file. If no path is specified, the file will be written to the directory from which the tool is run.
-h, --help, -?	Displays these command line switches and their functions

Figure 4: Windows* Console Tool Options

Following is an example of the **Intel-SA-00125-Console** output:

```
INTEL-SA-00125 Detection Tool
Application Version: <TOOL_VERSION>
Computer Name: <COMPUTER_NAME>
Scan date: <DATE_TIME>

*** Host Computer Information ***
Manufacturer: <MANUFACTURER_NAME>
Model: <MODEL_NAME>
Processor Name: <PROCESSOR>
OS Version: Microsoft Windows 10 Enterprise

*** Intel(R) ME Information ***
Engine: ME
Version: 11.0.18.1002
SVN: 1

*** Risk Assessment ***
Based on the analysis performed by this tool: This system is vulnerable.
Explanation:
The detected version of the Intel(R) Management Engine firmware is considered vulnerable for INTEL-SA-00125.
Contact your system manufacturer for support and remediation of this system.
For more information refer to the SA-00125 Detection Tool Guide or the Intel security advisory Intel-SA-00125 at the
following link: https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00125&languageid=en-fr
Saving results in: <APP_DIR>\SA-00125-<COMPUTER_NAME>L-YYYY-MM-DD-hh-mm.xml
```

Figure 5: Intel-SA-00125 Console Output Example

The following table describes the logic that is used to determine a risk assessment:

Message	Meaning
Vulnerable	The detected version of the Management Engine firmware is considered vulnerable for INTEL-SA-00125.
Not Vulnerable	The system meets the "Not Vulnerable" criteria described in *Identifying impacted systems using the INTEL-SA-00125 Detection Tool*
May Be Vulnerable	Tool could not communicate with the Intel® MEI/TXEI Driver. Platform vulnerability cannot be ascertained.
Unknown	The tool did not receive a valid response when requesting hardware inventory data from your computer. Contact the system manufacturer for assistance in determining the vulnerability of this system.

Figure 6: Risk Assessment Logic

3 Results

The amount of data returned by the Intel-SA-00125 Detection command depends on whether the Intel manageability driver stack is loaded onto the system. If the Intel® Management Engine Interface (Intel® MEI) driver is present, a more verbose set of data will be displayed. Some of the fields may not be supported by the manufacturer.

3.1 Registry Location

The values from the results table can be found in the following registry key:

HKLM\SOFTWARE\Intel\INTEL-SA-00125 Detection Tool.

Under this location, **System Status/System Risk** contains the vulnerability status and **System Status/System Risk Value** contains the application's return code.

3.2 XML

If you choose to write results to an XML file, that file will be stored in the directory from which you executed **Intel-SA-00125-console.exe** or in the path specified by the command line options. The results include information such as hardware inventory and OS. The filename will have the format **SA-00125-**<ComputerName>-<date>-<Time>.**xml**.

3.3 Console Return Codes

Number	Status	Meaning
0	NOTVULNERABLE | STATUS_OK	Platform is not vulnerable
10	HECI_NOT_INSTALLED	Intel® ME driver is not installed on the platform. Unable to determine platform vulnerability.
11	HECI_ERROR	Error communicating with the Intel® ME driver. Unable to determine platform vulnerability.
100	DISCOVERY_VULNERABLE_NOT_PATCHED	Platform is vulnerable.
101	DISCOVERY_NOT_VULNERABLE_PATCHED	Platform is not vulnerable, it has been patched
200	DISCOVERY_UNKNOWN	Unable to determine platform vulnerability

Figure 7: Console Return Codes

3.4 Console Output Values

Value	Location	Description
Application Version	Version of the scanning tool used	
Scan Date	Date and time of the scan	
Computer Name	Hardware inventory	Name of the computer scanned
Computer Manufacturer	Computer's manufacturer	
Computer Model	Computer's model	
Processor	Computer's processor model	
Engine	Intel® ME Firmware information	ME, CSME, TXE or SPS
ME Version	A string value with the full Intel® ME firmware version number in the following format: Major.Minor.Hotfix.Build	
SVN	Firmware Security Version Number	
*** Risk Assessment ***	Risk Assessment	Refer to Figure 6: Risk Assessment Logic

Figure 8: Console Output Values

4 Using the Intel SA-00125 Detection Tool to Identify Impacted Systems

Impacted systems are defined as those that have an affected Intel® Management Engine (ME) firmware version. The affected versions are listed in the following table:

	Vulnerable	Not Vulnerable
ME Version	Major ME version 11 and hotfix version lower than 55. Minor versions and build numbers are irrelevant. (E.g., 11.5.54.0 is vulnerable)	Major ME version 11 and hotfix version 55 or higher. Minor versions and build numbers are irrelevant. (E.g., 11.5.55.0 is not vulnerable)
TXE Version	Major TXE version 3 and hotfix version lower than 55. Minor versions and build numbers are irrelevant. (E.g., 3.0.54.0 is vulnerable)	Major TXE version 3 and hotfix version 55 or higher. Minor versions and build numbers are irrelevant. (E.g., 3.0.55.0 is not vulnerable)
SPS Version (both the operational and recovery versions must be checked for vulnerability)	Operational and Recovery Milestones <=4 For example: • SPS_E5_04.01.04.005.0 • SPS_E5_04.00.04.237.0 • SPS_E3_04.01.04.026.0	Operational and Recovery Milestone >=5 For example: • SPS_E5_04.01.05.001.0 • SPS_E5_04.00.05.001.0 • SPS_E3_04.01.05.001.0

Figure 9: Criteria for Determining Whether a System is Vulnerable

5 Troubleshooting Signature Validation Issues

The Detection tool makes every effort to validate its own authenticity before running.

In the event that the tool cannot validate itself, a message similar to the following will be displayed:

The signature of the file cannot be validated.Please refer to the INTEL-SA-00125 Detection Tool user guide for more information

Note: In case of a validation issue, you should ensure that the latest Root Certificate update for Windows* has been installed. For more information, refer to https://support.microsoft.com/en-us/help/931125/how-to-get-a-root-certificateupdate-for-windows