Intel-SA-00086 Detection Tool

User Guide

Revision 1.01
November 2017

Document: User Guide

Contents

Figures

Tables

§§

1 Introduction

This document will step you through multiple processes to detect the security vulnerability described in Intel-SA00086. Read the Public Security Advisory at https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086 for more information.

Table 1-1. Intel-SA-00086 CVE Entries – Search at https://nvd.nist.gov/vuln/search

Intel® Manageability Engine Firmware 11.0/11.5/11.6/11.7/11.10/11.20	CVE-2017-5705 CVE-2017-5708 CVE-2017-5711 CVE-2017-5712
Intel® Trusted Execution Engine 3.0	CVE-2017-5706 CVE-2017-5709
Server Platform Service 4.0	CVE-2017-5706 CVE-2017-5709

If you are a user of a single Windows* PC and you wish to determine its status: We provide the Intel-SA-00086 Detection GUI application (Intel-SA-00086-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-00086 Detection Tool console (Intel-SA-00086-console.exe) application. 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 provide the Intel-SA-00086 Detection console application (intel_sa00086.py) for analysis of Linux* systems.

§§

2 Using the Intel–SA–00086 Detection Tool

What is the Intel-SA-00086 Detection Tool?

The Intel-SA-00086 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-00086.

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

- For Windows* there is an interactive GUI tool that, when run, discovers the hardware and software details of the device and provides an indication of risk assessment. This version is recommended when local evaluation of a Windows* system is desired.
- 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 and/or text file. This version is more convenient for IT administrators wishing to perform bulk detection operations across multiple machines.

2.1 Obtaining the Intel-SA-00086 Detection Tool

The Intel-SA-00086 Detection Tool download package is available at:
https://downloadcenter.intel.com/download/27150

2.2 System Requirements

Windows*:

- Microsoft* Windows* 7, 8, 8.1, or 10 (Windows* 10S and Windows*10 IOT Core are not supported)
- Windows* 2012 R2 for servers (x64)
- .Net version 4.5 or later
- HECI Driver

Linux*:

- Ubuntu* LTS 16.0.4 (for client), Redhat 7.2 (for Server)

- Python* 2.7
- Local operating system administrative access

2.3 Installing the Tool – Linux*

- Unzip the package to a directory
- Insure that execute permission is set on the files:
  - intel_sa00086.py
  - spsInfoLinux64

2.4 Running the Linux* Console Tool

From the installation directory

Execute the command:

```
./intel_sa00086.py
```

Note: The Linux* tool takes no command line options

2.5 Installing the Tool – Windows*

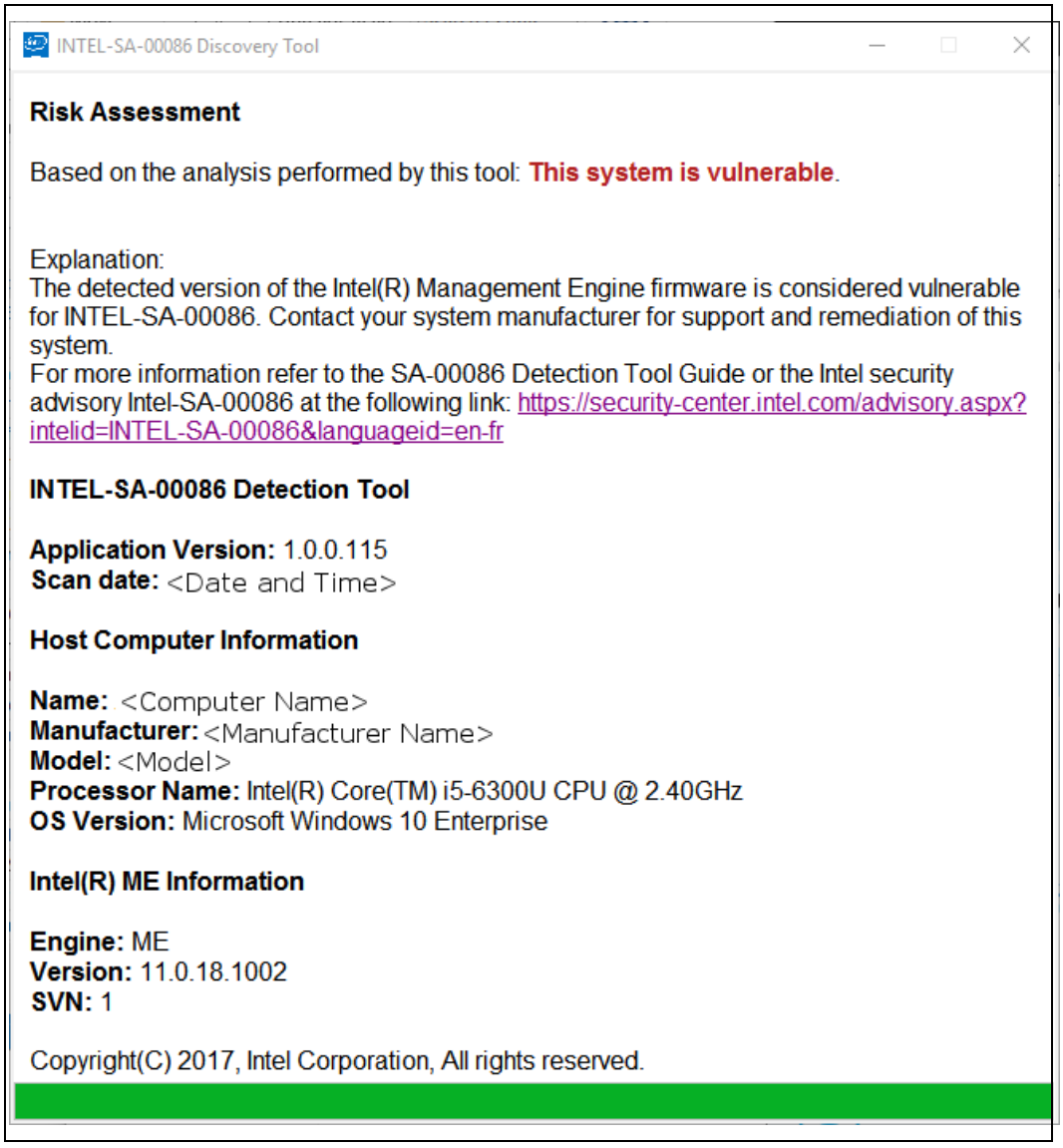
Unzip the downloaded package into a directory.

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-00086-GUI.exe is designed to run on a single system. When run, the tool outputs the detection information to the screen.

Figure 1. Example of Intel–SA–00086–GUI Output to Screen



***On SPS platforms the recovery version will be displayed in the ME Information section.**

2.7 Running the Windows* Console Tool

Execute **`INTEL-SA-00086-console.exe`** from a command prompt with administrative rights.

Usage:
`Intel-SA-00086-console.exe [[option...]]`

Table 2-1. Intel-SA-00086 Console Command Line Switches

Command Line Option	Functionality
-n, -noregistry	Prevents writing results to the registry
-c, -noconsole	Prevents results from being displayed on the console
-d, -delay <seconds>	Delay in seconds before execution starts. If no value is specified, the tool will have no delay.
-f, -writefile	Specifies writing results to a file. The filename uses the following format: <computername>.xml
-p <filepath>, -filepath <filepath>	The path to store the output file. If no path is specified, the file will be written to the directory that the tool is running from.
-h, -help, -?	Displays these command line switches and their functions

Figure 2. Example of Intel-SA-00086-Console Output

```
INTEL-SA-00086 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-00086.
Contact your system manufacturer for support and remediation of this system.
For more information refer to the SA-00086 Detection Tool Guide or the Intel security advisory Intel-SA-00086 at the
following link: https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr
Saving results in: <APP_DIR>\SA-00086-<COMPUTER_NAME>L-YYYY-MM-DD-hh-mm.xml
```

The logic used to determine a risk assessment is described in Table 2-2.

Table 2-2. Meaning of the Risk Assessment in the Output

Message	Meaning
Vulnerable	The detected version of the Management Engine firmware is considered vulnerable for INTEL-SA-00086.
Not Vulnerable	The system meets the “Not Vulnerable” criteria described in *Identifying impacted systems using the INTEL-SA-00086 Detection Tool*
Maybe Vulnerable	Tool could not communicate with the 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. • This message may be received on a server platform without a PMX Driver installed. This driver may be not available on all of versions of Windows* OS. If the driver is not present, the recommended workaround is to run spsInfo or spsManuf application provided with SPS Firmware release. Both applications will install the PMX Driver.

2.8 Results

Note: The amount of data returned by the Intel-SA-00086 Detection command will depend on if the Intel manageability driver stack is loaded on to the system. If the Intel® Management Engine Interface (MEI) driver is present there will be a more verbose set of data available. Some of the fields may not be supported by the manufacturer.

2.9 Registry Location

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

- `HKLM\SOFTWARE\`

  `Intel\Setup and Configuration Software\INTEL-SA-00086 Discovery Tool`

2.10 XML

If you choose to write results to an XML file, that file will be stored in the directory that Intel-SA-00086-console.exe is executed from or the path specified in the command line options. Information such as hardware inventory and OS is included.

2.11 Console Return Codes

Table 2-3. Intel-SA-00086 Console Return Codes

Number	Status	Meaning
0	NOTVULNERABLE | STATUS_OK	Platform is not vulnerable
10	HECI_NOT_INSTALLED	
11	HECI_ERROR	
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

Table 2-4. Intel-SA-00086 Console Output Values

Value	Location	Description
Application Version		The version of the scanning tool used
Scan Date		The date time the scan took place
Computer Name	Hardware Inventory	The name of the computer scanned
Computer Manufacturer		The computer's manufacturer
Computer Model		The computer's model
Processor		The computer's processor model
Engine	ME Firmware Information	ME, TXE or SPS
ME Version		A string value with the full ME firmware version number in the following format: Major.Minor.Hotfix.Build
SVN		Firmware Security Version Number
*** Risk Assessment ***	Risk Assessment	Refer Table 2-2

2.12 Identifying Impacted Systems Using the Intel-SA-00086 Detection Tool

Impacted systems are defined as having an affected Intel® Management Engine (ME) firmware version as defined in Table 2-5.

Table 2-5. Criteria to determine if a System is Vulnerable to Intel - SA-00086 Using the Intel-SA-00086 Detection Tool

	Vulnerable	Not Vulnerable
ME Version	ME Versions 11.x.x.x with SVN < 3	ME Versions: 11.8 and higher with SVN >=3
TXE Version	TXE Versions 3.0.x.x with SVN < 3	TXE Versions 3.1 and higher with SVN >=3
SPS Version NOTE: Both the operational and recovery versions must be checked for vulnerability	Operational and Recovery Milestones <=3 For example: • SPS_E5_04.01.03.005.0 • SPS_E5_04.00.03.237.0 • SPS_E3_04.01.03.026.0	Operational and Recovery Milestone >=4 For example: • SPS_E5_04.01.04.001.0 • SPS_E5_04.00.04.001.0 • SPS_E3_04.01.04.001.0

2.13 iCLS Health

In the event that the Detection tool finds problems with the iCLS configuration, it will print status messages as defined in Table 2-6

Table 2-6. iCLS Status Messages

Message	Action
Installed iCLS Client is obsolete. Minimum required version is 1.47.715.0. Update iCLS Client software.	• Update iCLS client software.
Service Intel® Capability Licensing Service TCP IP Interface is not installed. Install iCLS Client software.	• Insure iCLS client software is properly installed.
Service Intel® TPM Provisioning Service is not installed. Install iCLS Client software.	• Insure iCLS client is properly installed. Contact your OEM if problem persists.

Message	Action
Service Intel® TPM Provisioning Service is not running. Contact the OEM for support.	• Insure TPM Provisioning service is running. Contact your OEM if problem persists.
iCLS software is installed and healthy, but re-key has failed. Contact the OEM for support.	• Contact the OEM for support
Network is OK but iCLS Client may require HTTP proxy server settings to be configured in: "%%ProgramData%%\\Intel\\iCLS Client\\conf\\iclsProxy.conf". Note that iCLS Client does not support auto configuration scripts nor automatic proxy detection.	• Configure iCLS Client proxy server settings as specified in the message.
No connection to TCS Backend. Possible causes: • No network connection (Wi-Fi or other) • No access to https://ias.intel.com (blocked by firewall) • No HTTP proxy configured	• Check network connectivity and access to https://ias.intel.com.

§§