

INTEL-SA-00075 检测和缓解工具指南

英特尔®主动管理技术 (英特尔®AMT)、英特尔®标准管理 (ISM) 和英特尔®小企业技术 (SBT)

检测和缓解 INTEL-SA-00075 的说明

修订版 1.1 – 2017 年 7 月 20 日

简介

本文档将指导您完成多个进程，以检测和缓解 INTEL-SA-00075 中所述的安全漏洞。您可以阅读公共安全咨询 <https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr> 以获取更多信息。

如果您是单一电脑用户，并希望确定该机器的状态：我们提供对单一或独立系统进行本地分析的 INTEL-SA-00075 检测 GUI 应用程序 (Intel-SA-00075-gui.exe)。

如果您想要确定多台计算机的状态并/或执行威胁缓解步骤：我们提供了 INTEL-SA-00075 检测和缓解工具控制台 (Intel-SA-00075-console.exe) 应用程序。此工具可以执行发现，并将结果写入本地 Windows 注册表和 (可选) XML 文件中，以用于后续收集和分析。控制台应用程序还可帮助实施威胁缓解步骤。请参阅第 2 页 *使用 INTEL-SA-00075 检测和缓解工具* 了解详细信息。

如果您是网络管理员，且已在使用英特尔® 安装和配置软件 (英特尔® SCS)：英特尔® SCS 套件包含一款替代的控制台工具，英特尔® SCS 系统发现实用程序。如果您已经熟悉英特尔® SCS 工具或想要获取有关英特尔® 主动管理技术的详细数据，我们建议您使用此工具。请参阅第 10 页 *使用英特尔® SCS 系统检测实用工具*。

缓解

本文档中描述的缓解步骤旨在防止对尚未应用解决安全风险的更新的英特尔® 可管理性 SKU、英特尔® 主动管理技术 (英特尔® AMT)、英特尔® 标准管理 (ISM) 和英特尔® 小企业技术 (SBT) 的未经授权的激活和使用。

IT 工作人员可以将这些说明用作在管理控制台大规模部署缓解步骤的脚本或任务的基础。实施缓解的步骤如下所示：

1. 取消配置英特尔可管理性 SKU 的客户端以缓解未经授权的网络攻击者获得系统权限的风险
2. 禁用或移除本地可管理性服务(LMS)以缓解未经授权的本地攻击者获得系统权限的风险
3. 配置本地可管理性配置限制 (可选)

英特尔强烈建议：所有缓解路径中的第一步是取消配置英特尔可管理性 SKU 以解决网络权限提升漏洞。对已配置的系统，取消配置的操作必须在禁用或移除 LMS 之前进行。有待更新的英特尔可管理性 SKU 固件的推出，英特尔强烈建议移除或禁用 LMS 以缓解本地权限的提升。(可选) 作为防止意外重新安装或重新启用 LMS 的第二层防线，可以通过操作系统将一些由操作系统配置的可管理性配置选项进行额外的禁用：这些额外的本地可管理性配置限制对如何允许将其撤消有相应的约束。

注：主动管理技术 6.0.x 不支持主机基本资源配置/客户端控制模式，并因此不能由 INTEL-SA-00075 检测和缓解工具通过本地操作系统接口取消配置。对使用可管理性固件 6.0.x.x 或 6.1.x.x 6.0 的平台，有必要使用英特尔 SCS 套件的 ACUConfig /full 或通过系统 MEBx 完全取消配置。

若要就实施本文档中提供的缓解步骤获得帮助，请联系[英特尔客户支持](#)；在技术部分中选择英特尔® 主动管理技术 (英特尔® AMT)。

使用 INTEL-SA-00075 检测和缓解工具

INTEL-SA-00075 检测和缓解工具是什么？

本地用户或 IT 管理员可使用 INTEL-SA-00075 检测和缓解工具来确定系统是否可能受到英特尔安全通报 INTEL-SA-00075 中所描述的攻击。工具的控制台版可用来执行缓解步骤。

检测和缓解工具提供两个版本。

- 第一个版本使用交互式图形用户界面，检测设备的软硬件的详细信息并提供风险评估。此版本用于单台电脑的本地检测。
- 第二个版本是控制台可执行文件，它可以执行风险评估，并执行可建议的缓解步骤。它也可以将发现信息存储至 Windows * 注册表和/或 XML 文件中。此版本对希望在多台计算机上执行批量发现和缓解操作的 IT 管理员来说更为方便。

获取 INTEL-SA-00075 检测和缓解工具

INTEL-SA-00075 检测和缓解工具的下载包可从此网址获得：

<https://www.intel.com/content/www/cn/zh/support/technologies/000024133.html>。

系统要求

- Microsoft Windows* 7、8、8.1 或 10
- 本地操作系统的管理员权限

安装该工具

交互式安装

运行 INTEL-SA-00075 检测和缓解工具，并按照屏幕上的提示进行操作。

静默安装

```
msiexec.exe /i INTEL-SA-00075 Detection and Mitigation Tool.msi /qn
```

这将在默认目录中安装 INTEL-SA-00075 检测和缓解工具，
C:\Program Files (x86)\Intel\Intel-SA-00075 Detection and Mitigation Tool\

卸载该工具

交互式卸载

运行 INTEL-SA-00075 检测和缓解工具，并按照屏幕上的提示操作。

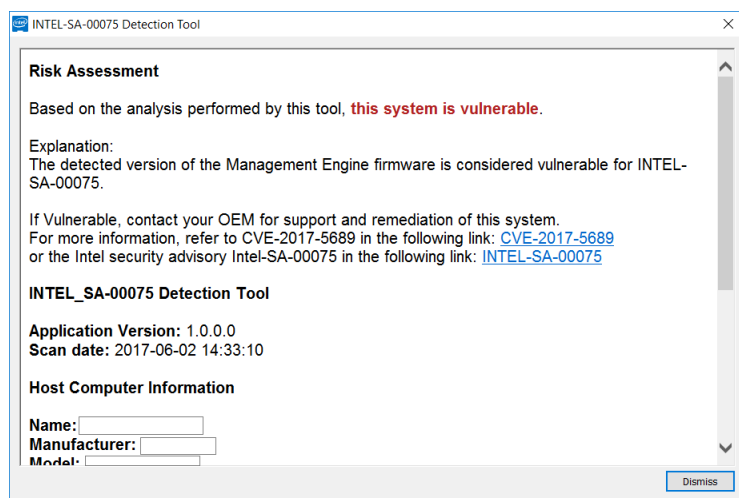
静默卸载

```
msiexec.exe /x INTEL-SA-00075 Detection and Mitigation Tool.msi /qn
```

运行该工具的图形用户界面版本

INTEL-SA-00075-gui.EXE 可在单一系统上运行。检测结果将显示在屏幕上。

图 1 INTEL-SA-00075 图形用户界面版本的屏幕显示



运行控制台可执行程序

在管理员权限下从命令提示符运行 INTEL-SA-00075-console.exe。

用法：

Intel-SA-00075-console.exe [[命令] | [选项...]]

每次仅可运行一条命令。如果不给出任何命令，则运行 discover 命令。

表 1. INTEL-SA-00075 控制台命令选项

命令行命令	功能
-Discover	将结果输出到控制台，并将数据写入注册表。
-Unprovision [password], -u [password]	删除所有英特尔 AMT 设置并禁用英特尔® AMT 功能；可使用可能是必需的英特尔® AMT 设备管理员用户密码。 注意：不用密码而调用此命令仅适用于受 INTEL-SA-00075 (6.1.x.x-11.6.x.x，其内部版本号为 3000 以下) 影响的固件版本。如果使用内部版本号大于 3000 的固件版本 6.1.x.x-11.6.x.x，取消配置仅在提供密码后才能工作。
-DisableClientControlMode, -DisableCCM	永久禁用英特尔 AMT 设备中的客户端控制模式选项。运行此命令后，设备不能再进入客户端控制模式。注意：没有用以撤消此操作的 CLI 命令。 警告：并非所有的平台都可以在 CCM 被禁用后再重新启用。
-DisableLMS	禁用 LMS 服务。

命令行选项	功能
-n, -noregistry	检测结果不写入注册表
-c, -noconsole	检测结果不显示在控制台上
-d, -delay <seconds>	显示开始执行以前延迟的秒数。如果不指定任何值，该工具将无延迟。
-f, -writefile	将检测结果写入一个文件。文件名使用以下格式：<computername>.xml
-p <filepath>, -filepath <filepath>	输出文件的路径。如果不指定路径，则默认使用与检测工具相同的目录。
-h, -help, -?	显示以上命令行选项和功能

-Discover

Discover 命令将发现信息输出到控制台。默认情况下它还将发现数据写入注册表。如果不向控制台工具发出任何命令，便运行 discover 命令。

-Unprovision

删除所有英特尔 AMT 设置并禁用英特尔® AMT 功能；可以对英特尔® AMT 设备使用可选的管理员用户密码。

一旦配置，英特尔® AMT 和 ISM 便自动侦听计算机网络上的管理通讯。对易受已知的权限提升问题攻击的系统应该使用 unprovision 命令来取消配置，以防止对可管理性功能的未经授权的访问。

不用密码而调用此命令仅适用于受 INTEL-SA-00075 (6.1.x.x-11.6.x.x，其内部版本号为 3000 以下) 影响的固件版本。如果使用内部版本号大于 3000 的固件版本 6.1.x.x-11.6.x.x，取消配置仅在提供密码后才能工作。

-DisableClientControlMode

-DisableClientControlMode 配置限制是要求有第二层保护以防止获得了操作系统管理权限的未经授权的攻击者进行缓解恢复的客户的可选步骤。恢复这些选项很难，计算机制造商可能不支持，并且可能需要对系统进行物理访问。如果您选择要执行此额外的配置限制，则必须在禁用 LMS 服务之前执行。

重新启用 CCM 的步骤

如果您的制造商支持，您可以从 BIOS 重置英特尔可管理性 SKU，这将重新启用 CCM。请咨询您的制造商，以确定他们是否支持此功能，并了解操作步骤。

注：您的制造商可能会提供工具，使您可以通过操作系统配置 BIOS 的设置。这些工具，如果可用，可能会允许您在 BIOS 中重置英特尔可管理性 SKU，而无需实际接触计算机。请咨询您的制造商，了解他们是否提供具备此功能的工具。

-DisableLMS

DisableLMS 命令禁用 LMS 服务，作为一个缓解步骤。

什么是 LMS？

英特尔® 管理和安全应用程序本地管理服务 (LMS) 是一项服务，使在英特尔® AMT、英特尔® SBA 或英特尔® 标准可管理性支持的设备上运行的本地应用程序能使用通用的 SOAP 和 WS 管理功能。它会侦听英特尔® 可管理性引擎 (ME) 端口 (16992、16993、16994、16995、623 和 664) 并将通讯通过英特尔® MEI 驱动程序路由到固件。

其他考虑因素

具有操作系统管理权限的任何人都可以重新安装 LMS (如果已被删除)，或重新启用此服务 (如果已被禁用)。因此，操作中务必谨慎，以避免在系统存在安全漏洞的情况下意外重新安装或重新启用 LMS。例如，如果您在未来的某个时候运行英特尔可管理性软件，便可以重新安装 LMS。

图 2. INTEL-SA-00075 控制台输出示例

```
INTEL-SA-00075 检测工具
应用程序版本: <应用程序版本>
扫描日期: <日期和时间>

*** 主机计算机信息 ***
计算机名称: <计算机名称>
制造商: <计算机制造商>
型号: <计算机型号>
处理器: <处理器型号>
Windows 版本: <windows* 版本>

*** ME 信息 ***
版本: <英特尔 ME 固件版本>
SKU: <可管理性功能, 如果存在>
状态: <ME 配置状态>
安装的驱动程序: <True/false>
控制模式: <无/ACM/CCM>
CCM 禁用: <True/false/未知>
EHBC 启用 <True/False>
LMS 状态: <运行/停止/不存在>
LMS 启动类型: <启动/系统/自动/手动/禁用/NotPresent>
MicroLMS 状态: <运行/停止/不存在>
MicroLMS 启动类型: <启动/系统/自动/手动/禁用/NotPresent>
是 SPS: <True/False>

*** 风险评估 ***
基于此工具进行的分析,
< 该系统易受攻击 /
```

此系统不易受攻击 /
 此系统不易受攻击；非英特尔 SKU /
 此系统不易受攻击；ME FW 版本不受影响 /
 此系统不易受攻击；ME SKU 不受影响 /
 此系统不易受攻击；SMBIOS 表明这是消费者 SKU /
 此系统不易受攻击；系统正在运行 SPS FW (服务器平台服务固件) /
 此系统的固件已更新，系统处于未配置状态 /
 该系统的固件已更新，系统处于配置状态 /
 请联系 OEM /
 该系统的风险未知 >

如果受到攻击，请联系 OEM 以获取此系统的支持和修复。

*** 更多信息 ***

请参阅 CVE-2017-5689:

<https://nvd.nist.gov/vuln/detail/cve-2017-5689>

或参阅英特尔安全咨询 Intel-SA-00075:

<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr>

用来确定风险评估的逻辑在表 2 中说明。

表 2. 输出的风险评估的意思

消息	表示的意思
受影响	检测到的管理引擎固件版本视为对 INTEL-SA-00075 易受攻击。
不受影响	系统符合第 8 页上 使用 INTEL-SA-00075 检测工具甄别受影响的系统中所述的“不易受攻击”标准。
该系统的固件已更新，系统处于未配置状态	在此系统上的检测到的固件有适用于 INTEL-SA-00075 的修复。确保在重新配置之前使用 INTEL-SA-00075 工具对系统执行完全取消配置。这将删除所有未经授权的配置设置。
该系统的固件已更新，并且系统处于已配置状态	在此系统上的检测到的固件有适用于 INTEL-SA-00075 的修复。如果系统在固件更新之前已配置，则系统的完全取消配置和重新配置将删除所有未经授权的配置设置。
请联系 OEM	从 OEM 的 SMBIOS 中检测到的信息显示可管理性 SKU，但是该工具在请求计算机详细信息时未收到响应。这可能是由于未安装 AMT、ISM 或 SBT 的接口驱动程序。请联系您的生产商以确认您的计算机型号是否受影响。
未知的	此工具在请求计算机硬件清单时未能获得有效的响应。请联系您的系统制造商以获得帮助，以确定此系统的漏洞。 可能会在没有安装 PMX 驱动程序的服务器平台上收到此消息。此驱动程序可能不是在所有版本的 Windows 操作系统上都可用。如果该驱动程序不存在，则建议采用的解决方法是运行 SPS 固件版本附带 spsInfo 或 spsManuf 应用程序。两个应用程序都能安装 PMX 驱动程序。

结果

注意：INTEL-SA-00075 发现命令返回的数据量取决于英特尔可管理性驱动程序堆栈是否是否已加载到系统上。如果英特尔®管理系统接口 (MEI) 驱动程序和英特尔®本地管理服务 (LMS) 的管理和安全应用程序已加载，那么检测工具将显示更为详尽的信息。某些生产商或不支持某些数据信息。

注册表位置

检测结果保存在以下注册表项中:

- 32 位操作系统: HKLM\SOFTWARE\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool
- 64 位操作系统: HKLM\SOFTWARE\WOW6432Node\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool

XML

如果您选择将结果写入 XML 文件, 该文件将保存在与执行 INTEL-SA-00075-Console.exe 的相同目录内或在命令行选项中指定的路径中。将包括关于硬件清单、操作系统和 LMS 的存在等信息。如果 AMT 存在, 则将包括发现的默认和自定义证书哈希值列表。此列表可用于根据 AMT 所存储的内容审核预期的哈希值。

控制台返回代码

表 3. INTEL-SA-00075 控制台返回代码

号码	表示的意思
0	NOTVULNERABLE (If Discover command was run) STATUS_OK
2	MACHINE_STATE_UNCONFIGURED
30	CLIENT_CONFIG_NOT_SUPPORTED
39	DISABLE_CCM_IN_ADMIN_MODE
83	HECI_NOT_INSTALLED
111	HECI_ERROR
500	DISCOVERY__VULNERABLE
501	DISCOVERY_POTENTIALLYVULNERABLE_PROVISIONED
502	DISCOVERY_POTENTIALLYVULNERABLE_UNPROVISIONED
503	DISCOVERY_CHECKWITHOEM
504	DISCOVERY_UNKNOWN_RISK
505	DISCOVERY_UNKNOWN
506	DISCOVERY_UNKNOWN_CPU

表 4. INTEL-SA-00075 控制台输出值

值	位置	说明
Application Version (应用程序版本)		检测工具的版本
Scan Date (扫描日期)		检测工具运行的日期和时间
Computer Name (计算机名称)		已检测的计算机的名称
Computer Manufacturer (计算机制造商)	硬件清单	计算机制造商
Computer Model (计算机型号)		计算机型号
处理器		计算机的处理器型号
ME Version (ME 版本)	ME 固件信息	带有完整 ME 固件版本号的字符串值, 格式如下: Major.Minor.Hotfix.Build
ME SKU (ME 型号)		系统可管理性功能, 如果存在
ME Provisioning State (ME 配置状态)		ME 配置状态: 未检测到配置状态 未配置 正在配置 已配置
ME Driver Installed (已安装的)		True/False 值: 是否已安装 MEI 驱动程序

ME 驱动程序)		
EHBC Enabled (启用 EHBC)		True/False 值：系统是否支持嵌入式基于主机的配置方法
LMS State (LMS 状态)		LMS Service 正在运行、未运行、或不存在
LMS startup type (LMS 启动类型)		关于 LMS 启动类型是否为 NotPresent、引导、系统、自动、手动或禁用的信息
MicroLMS state (MicroLMS 状态)		关于 MicroLMS Service 是在运行、未运行，还是不存在的信息
MicroLMS startup type (MicroLMS 启动类型)		关于 MicroLMS 启动类型是否为 NotPresent、引导、系统、自动、手动或禁用的信息
Control Mode (控制模式)		ME 配置模式 无、ACM 或 CCM
Is CCM Disabled (CCM 禁用)		True/False/Unknown 值：客户控制模式已禁用
Is SPS (是 SPS)		平台是否为不易受攻击的服务器平台服务 (SPS) 系统？
*** 风险评估 ***	风险评估	参阅 表 2. 输出的风险评估的意思

使用INTEL-SA-00075检测工具甄别受影响的系统

受影响的系统定义为：安装有受影响的管理引擎 (ME) 固件版本，并包含 表5 中定义的三种功能之一。

注：服务器平台服务 (SPS) 平台就 INTEL-SA-00075 而言不易受到攻击。SPS 平台有在服务器平台上的可管理性引擎 (ME) （属于 PCH ）上运行的固件。该固件不同于在 PC/工作站平台上运行的英特尔可管理性固件（也在 ME 上运行）。

表 5. 使用 INTEL-SA-00075 发现工具确定系统是否就 INTEL-SA-00075 而言易受攻击

值名称	受影响	不受影响
ME SKU (ME 型号)	Intel® Full AMT Manageability Intel® Standard Manageability Intel® Small Business Advantage (SBA)	ME SKU 值未出现在左边的受影响列表 或 ME SKU 值出现在左边的受影响列表，但固件版本显示为不受影响
ME Version (ME 版本)	ME 固件版本 6.x.x.x-11.7.x.x，且第四个数字小于 3000 例如 9.5.22. 1760	ME 固件版本： <ul style="list-style-type: none">6.x.x.x-11.7.x.x 且第四个数字大于或等于 3000<ul style="list-style-type: none">例如：11.6.27.32642.x.x.x。 – 5.x.x.x11.7.x.x 或更高版本

注：英特尔®小企业技术(SBT)是英特尔® 中小企业通锐(SBA) 的可管理性 SKU。

扩展 Microsoft* SCCM 硬件清单以涵盖 INTEL-SA-00075 控制台工具的结果

如果您选择把 Intel-SA-00075 控制台工具的结果存储在 Windows 注册表中， 您可以利用微软® SCCM 硬件清单的可扩展性导入检测结果。这使您能在 SCCM 里建立对目标计算机的漏洞修补或固件更新。要执行此操作， 您需要以下步骤：

1. 将硬件清单类添加到 SCCM configuration.mof 文件中。
2. 在客户端设置中启用新硬件清单类。
3. 创建软件包以部署和运行 INTEL-SA-00075 控制台工具 (Intel-SA-00075-console.exe)。
4. 创建一个任务序列来运行这个软件包。

MOF 文件的修改

注意：如果您的网络环境中有一台中央服务器，请在中央服务器上修改 MOF 文件。否则，则要在每一台一级服务器上修改 MOF 文件。

1. 找到configuration.mof 文件。它通常位于 \Program Files\Microsoft Configuration Manager\inboxex\clifiles.src\hin\
2. 创建一个备份副本。
3. 编辑 configuration.mof 文件。向下滚动到文件的末尾，将光标停在这些注释之上：

```
//=====
// Added extensions end
//=====
```

4. 将本文档第 13-14 页上的 MOF 文件更改内容粘贴到步骤三的上行。
5. 保存并关闭该文件。
6. 在管理员权限下启动一个命令提示符窗口，进入 configuration.mof 所在的目录。
7. 对修改后的configuration.mof运行mofcomp，无命令行开关项。

硬件清单的更改

注：一旦作出变更，它们将需要一些时间才能出现客户端上，然后这些新条目将出现在硬件清单中。这个过程需要的时间长短取决于环境的配置方式。

1. 创建一个名为 INTEL-SA-00075.mof 的新文件。
2. 将第 15 页上的 INTEL-SA-00075 硬件清单导入 内容插入新创建的文件，并保存。
3. 启动 Configuration Manager Console
4. Administration > Client Settings > Default Client Settings。
5. 右键单击 Default Client Settings > Properties。
6. 选择 Hardware Inventory > Set Classes。
7. 单击 导入。
8. 导航至 INTEL-SA-00075.mof 文件 > 打开。
9. 确认已选择“导入硬件清单类和硬件清单类设置”选项。
10. 单击 导入。
11. OK > OK。
12. SCCM 将硬件清单的更改记录在 dataldr.log 文件中。

创建 SCCM 软件包

1. 从第 15 页创建一个批处理文件，将此批处理文件置于 INTEL-SA-00075 控制台工具文件的同一个目录下。
2. 启动 Configuration Manager Console
3. Software Library > Packages。
4. 右键单击 Packages > Create Package。
5. 名称：Intel-SA-00075。
6. 检查此软件包是否包含源文件。
7. 进入软件包目录（第一步）
8. Next。

9. 选择 Do not create a program。
10. Next > Next > Close。
11. 将软件包分发给相应的分发点。

创建 SCCM 任务序列

1. 启动 Configuration Manager Console
2. Software Library > Operating Systems。
3. 右键单击 Task Sequences > Create Task Sequence。
4. 选择 Create a new custom task sequence。
5. Next。
6. 输入名称: Intel-SA-00075。
7. Next > Next > Close。
8. 右键单击 Intel-SA-00075 任务序列, 然后单击 Edit。
9. Add > General > Run Command Line。
10. 在 Command Line 一栏中输入 Intel-SA-00075.bat
11. 勾选 Package 框并选择 Browse。
12. 选择刚才创建的 Intel-SA-00075 软件包 > OK。
13. 点击 OK。

使用英特尔® SCS 系统检测实用工具

英特尔® SCS 系统检测实用工具是什么？

英特尔® SCS 系统检测实用工具是英特尔®安装和配置软件套件(SCS)的一个组件。此工具向您提供支持英特尔®主动管理技术(英特尔® AMT)、英特尔®标准管理(ISM)、或英特尔®小企业技术(SBT)的系统的某些软硬件详细信息。运行结果可以保存在微软 Windows 注册表或一个 XML 文件里。此信息可用于查找那些需要固件更新或安装补丁的计算机。

获取英特尔® SCS 系统检测实用工具

英特尔® SCS 系统发现实用程序的下载包可从以下网址获得：

<https://downloadcenter.intel.com/download/26691/Intel-SCS-System-Discovery-Utility>。

用英特尔® SCS 系统检测实用工具来确定 ME 固件的版本

英特尔® SCS 系统发现实用工具输出的信息可用于确定系统的固件版本以及系统是否支持 AMT、ISM、或 SBT。英特尔® SCS 系统检测实用工具输出信息中的 Manageabilityinfo 部分中提供此信息。有关运行此工具的说明, 请参阅第 12 页上的 *运行英特尔® SCS 系统检测实用工具* 部分。

FWVersion 值显示计算机当前运行的固件版本。AMTSKU 值 (若显示) 包含计算机所支持可管理型号。查看 FWVersion 和 AMTSKU 以确定您的系统的漏洞, 如表 6 所描述。

表 6. 使用 Intel® SCS 系统发现实用程序来确定系统是否对 INTEL-SA-00075 而言易受攻击。

值名称	受影响	不受影响
AMTSKU	Intel® Full AMT Manageability Intel® Standard Manageability Intel® Small Business Advantage (SBA) 输出示例 <ManageabilityInfo> <AMTSKU>Intel(R) Full AMT Manageability</AMTSKU> <AMTversion>11.0.0</AMTversion> <FWVersion>11.0.0.1202</FWVersion>	AMTSKU 值未出现在左边的受影响列表 或 AMTSKU 值出现在左边的受影响列表，但固件版本显示为不受影响 输出示例 <ManageabilityInfo> <FWVersion>9.0.13.1402</FWVersion>
FWVersion	ME 固件版本 6.x.x.x-11.7.x.x，且第四个数字小于 3000 例如 9.5.22. <u>1760</u>	ME 固件版本： <ul style="list-style-type: none">6.x.x.x-11.7.x.x 且第四个数字大于或等于 3000<ul style="list-style-type: none">例如：11.6.27.<u>3264</u>2.x.x.x₀ – 5.x.x.x11.7.x.x 或更高版本

注：英特尔®小企业技术(SBT)是英特尔® 中小企业通锐(SBA)的可管理性 SKU。

运行英特尔® SCS 系统发现实用工具

数据仅保存到注册表中

以管理员权限在命令提示符窗口运行以下命令，以运行英特尔®系统 SCS 发现工具并将数据写入注册表中：

```
SCSDiscovery.exe SystemDiscovery /nofile
```

数据仅保存到一个 XML 文件中

使用以下命令以运行英特尔® SCS 系统发现实用工具，并将数据保存为一个 XML 文件：

```
SCSDiscovery.exe SystemDiscovery <文件名和路径> /noregistry
```

“文件名和路径”可以是本机的也可以位于网络共享。如果您选择使用网络共享，请确保运行英特尔® SCS 系统发现实用工具的账号对该网络共享拥有写权限。如果不指定文件名和路径，系统的完全合格域名（ FQDN ）将用于命名该XML文件；该XML文件将存储在与英特尔® SCS 系统发现实用工具相同目录下。

数据保存到注册表和XML文件

使用以下命令以运行英特尔® SCS 系统发现实用工具，并将数据保存到注册表以及一个 XML 文件中

```
SCSDiscovery.exe SystemDiscovery <文件名和路径>
```

如前所述，如果不指定文件名和路径，系统的完全合格域名（ FQDN ）将用于命名该XML文件；该XML文件将存储在与英特尔® SCS 系统发现实用工具相同目录下。

英特尔® SCS 系统发现实用工具的运行结果

英特尔® SCS 系统发现实用工具所返回的数据量取决于英特尔可管理系统的驱动程序是否已加载。如果英特尔®管理系统接口 (MEI) 驱动程序和英特尔®本地管理服务 (LMS) 的管理和安全应用程序已加载，那么检测工具将显示更为详尽的信息。以下描述着重于与已知的权限升级问题相关的若干关键数据。想要获取其他数据的更多信息，请参阅英特尔® SCS 系统发现实用工具文档。某些生产商或不支持某些数据

信息。

注册表的结果

保存到注册表的结果位于以下位置：
HKLM\Software\Intel\Setup and Configuration Software\SystemDiscovery

关键数值：

值名称	注册表子键	值说明
FWVersion	ManageabilityInfo	英特尔®管理引擎固件版本
AMTSKU	ManageabilityInfo	受支持的可管理性功能，如果存在

系统所支持的管理功能（若存在）

XML®管理引擎固件版本位于 XML 中的以下路径：

```
<SystemDiscovery>
  <ManageabilityInfo>
    <FWVersion> 版本号 </FWVersion>
```

系统所支持的管理功能（若存在）位于 XML 中的以下路径：

```
<SystemDiscovery>
  <ManageabilityInfo>
    <AMTSKU> 管理功能名称 </AMTSKU>
```

将系统发现数据导入SCCM 硬件清单

收集系统发现数据的过程可通过微软®系统中心配置管理器 (SCCM)的英特尔® SCS 插件实现自动化。一旦安装此插件，它将自动扩展 SCCM 硬件清单，以涵盖系统发现数据并创建用于运行系统发现的任务序列。此过程收集的信息可用于创建 SCCM 集合，以在受影响的系统上更新固件或安装补丁。

微软® 系统中心配置管理器 (SCCM) 的英特尔® SCS 插件软件包可从以下网址获得：
<https://downloadcenter.intel.com/download/26506/Intel-SCS-Add-on-for-Microsoft-System-Center-Configuration-Manager>.

MOF 文件的更改

```
//===== Intel-SA-00075 Start =====

#pragma namespace ("\\\\.\\root\\cimv2")
#pragma deleteclass("INTEL_SA_00075_ME_Information", NOFAIL)
[DYNPROPS]
Class INTEL_SA_00075_ME_Information
{
  [key] string KeyName;
  String MEVersion;
  UInt32 MEVersionMajor;
  UInt32 MEVersionMinor;
  UInt32 MEVersionBuild;
  UInt32 MEVersionRevision;
```

```
String MEDriverInstalled;
String MESKU;
String MEProvisioningState;
String LMSPresent;
String MicroLMSPresent;
String IsCCMDisabled;
String ControlMode;
String EHBCEnabled;
};

[DYNPROPS]
Instance of INTEL_SA_00075_ME_Information
{
  KeyName="INTEL-SA-00075";
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version"),Dynamic,Provider("RegPropProv")] MEVersion;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version Major"),Dynamic,Provider("RegPropProv")] MEVersionMajor;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version Minor"),Dynamic,Provider("RegPropProv")] MEVersionMinor;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version Build"),Dynamic,Provider("RegPropProv")] MEVersionBuild;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version Revision"),Dynamic,Provider("RegPropProv")] MEVersionRevision;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Driver Installed"),Dynamic,Provider("RegPropProv")] MEDriverInstalled;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME SKU"),Dynamic,Provider("RegPropProv")] MESKU;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Provisioning State"),Dynamic,Provider("RegPropProv")] MEProvisioningState;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|LMS Present"),Dynamic,Provider("RegPropProv")] LMSPresent;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|Micro LMS Present"),Dynamic,Provider("RegPropProv")] MicroLMSPresent;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|Is CCM Disabled"),Dynamic,Provider("RegPropProv")] IsCCMDisabled;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|Control Mode"),Dynamic,Provider("RegPropProv")] ControlMode;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|EHBC Enabled"),Dynamic,Provider("RegPropProv")] EHBCEnabled;
};

//===== Intel-SA-00075 End =====
```

INTEL-SA-00075 硬件清单导入

```
#pragma namespace ("\\.\root\cimv2\SMS")
#pragma deleteclass("INTEL_SA_00075_ME_Information", NOFAIL)
[SMS_Report(TRUE),SMS_Group_Name("INTEL_SA_00075_ME_Information"),SMS_Class_ID("INTEL_SA_00075_ME_Information"),
SMS_Context_1("__ProviderArchitecture=32|uint32"),
SMS_Context_2("__RequiredArchitecture=true|boolean")]
Class INTEL_SA_00075_ME_Information: SMS_Class_Template
{
[SMS_Report(TRUE),key] string KeyName;
[SMS_Report(TRUE)] String MEVersion;
[SMS_Report(TRUE)] UInt32 MEVersionMajor;
[SMS_Report(TRUE)] UInt32 MEVersionMinor;
[SMS_Report(TRUE)] UInt32 MEVersionBuild;
[SMS_Report(TRUE)] UInt32 MEVersionRevision;
[SMS_Report(TRUE)] String MEDriverInstalled;
[SMS_Report(TRUE)] String MESKU;
[SMS_Report(TRUE)] String MEProvisioningState;
[SMS_Report(TRUE)] String LMSPresent;
[SMS_Report(TRUE)] String MicroLMSPresent;
[SMS_Report(TRUE)] String IsCCMDisabled;
[SMS_Report(TRUE)] String ControlMode;
[SMS_Report(TRUE)] String EHBCEnabled;
};
```

INTEL-SA-00075.bat 批处理文件

```
@echo off
.\Intel-SA-00075-console
SET EL=%ERRORLEVEL%
rem Schedule HW inventory
SET HWInventoryGUID="{00000000-0000-0000-0000-000000000001}"
wmic /IMPLEVEL:Impersonate /AUTHLEVEL:Pktprivacy /namespace:\\root\ccm path sms_client CALL
TriggerSchedule %HWInventoryGUID% /NOINTERACTIVE
echo Exit code: %EL%
exit %EL%
```

收集查询示例

已配置的计算机

```
select * from SMS_R_System inner join SMS_G_System_INTEL_SA_00075_ME_Information on
SMS_G_System_INTEL_SA_00075_ME_Information.ResourceID = SMS_R_System.ResourceId where
SMS_G_System_INTEL_SA_00075_ME_Information.MEProvisioningState = "Provisioned"
```

LMS 已运行

```
select * from SMS_R_System inner join SMS_G_System_INTEL_SA_00075_ME_Information on
SMS_G_System_INTEL_SA_00075_ME_Information.ResourceID = SMS_R_System.ResourceId where
```

```
SMS_G_System_INTEL_SA_00075_ME_Information.LMSPresent = "Running" or  
SMS_G_System_INTEL_SA_00075_ME_Information.MicroLMSPresent = "Running"
```

本文档所提供之信息均与英特尔® 产品相关。本文未授与任何知识产权方面的特许，无论是明示还是暗示、禁止反言或者其它方式。除相关产品的英特尔销售条款与条件中列明之担保条件以外，英特尔公司不对销售和/或使用英特尔产品做出任何其它明确或隐含的担保，包括对适用于特定用途、适销性，或不侵犯任何专利、版权或其它知识产权的担保。除非经英特尔书面同意，英特尔产品并非设计用于或有意用于任何英特尔产品发生故障可能会引起人身伤亡事故的应用领域。

英特尔技术的特性和优势取决于系统配置，并且可能需要激活相应的硬件、软件或服务。其性能可能因系统配置的不同有所差异。没有计算机系统是绝对安全的。请咨询您的系统制造商、零售商或访问 intel.com 了解更多信息。

版权所有 © 2017，英特尔公司。保留所有权利。英特尔和英特尔标识是英特尔公司在美国和其他国家(地区)的商标。

* 其它名称和品牌可能由其它公司所拥有。