

INTEL-SA-00075 — Руководство по обнаружению и устранению уязвимостей

Технология Intel® Active Management Technology (Intel® AMT), функции Intel® Standard Manageability (ISM) и технология Intel® Small Business Technology (SBT)

INTEL-SA-00075 — Инструкции по обнаружению и устранению уязвимостей

Редакция 1.1 – 20 июля 2017 г.

Введение

В этом документе представлено несколько действий, которые необходимо выполнить для обнаружения и устранения системной уязвимости, описанной в статье INTEL-SA-00075. Для получения дополнительной информации ознакомьтесь с рекомендациями по общественной безопасности на странице <https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr>.

Если вы используете всего один компьютер и хотите определить его статус: мы предлагаем использовать интерфейс приложения обнаружения, INTEL-SA-00075 (Intel-SA-00075-gui.exe), для выполнения анализа одной или автономной системы.

Если вы хотите определить статус и/или применить исправления для нескольких компьютеров: мы предлагаем вам воспользоваться приложением консоли (Intel-SA-00075-console.exe) для обнаружения и устранения уязвимости, представленной в статье INTEL-SA-00075. Это приложение может выполнять обнаружение и запись результатов в локальный реестр Windows и файл XML (дополнительно) для их последующего сбора и анализа. Приложение консоли также может использоваться для устранения уязвимости. См. *Использование приложения обнаружения и устранения уязвимости*, INTEL-SA-00075 на стр. 2 для получения дополнительной информации.

Если вы являетесь сетевым администратором и используете приложение Intel® SCS (Intel® Setup and Configuration Software): комплект приложения Intel® SCS содержит альтернативу консоли, а именно, приложение Intel® SCS Intel® SCS System Discovery Utility. Мы рекомендуем использовать это приложение, если вы уже знакомы со средствами Intel® SCS или хотели бы получить подробные данные о характеристиках технологии Intel® AMT. См. *Использование приложения Intel® SCS System Discovery Utility* на стр. 121.

Устранение уязвимости

Действия устранения уязвимости, которые представлены в этом документе, предназначены для предотвращения несанкционированного включения и использования SKU с функциями управления Intel, технологии Intel® Active Management (Intel® AMT), функций ПО Intel® Standard Manageability (ISM) и технологии Intel® Small Business (SBT), которые не устанавливают обновление встроенного ПО, используемое для устранения этой уязвимости.

ИТ-специалисты могут воспользоваться этими инструкциями в качестве основы для создания сценариев или задач, выполняемых на консолях управления для крупномасштабных развертываний с действиями по устранению уязвимостей.

Действия процедур устранения уязвимости:

1. Отмена настроек клиентских SKU с функциями управления Intel для устранения возможностей злоумышленников получения системных привилегий.
2. Отключение или удаление службы локального управления LMS (Local Manageability Service) для предотвращения получения злоумышленниками системных привилегий.
3. Дополнительная конфигурация локальных ограничений настроек функций управления.

Корпорация Intel настоятельно рекомендует использовать в качестве первого действия для всех процедур устранения уязвимостей отмену настроек SKU с функциями управления Intel для устранения возможности эскалации сетевых привилегий. Для подготовленных систем отмена настроек должна выполняться до отключения или удаления функций локального управления LMS. Несмотря на возможность использования обновленного встроенного ПО для SKU с функциями управления Intel, корпорация Intel настоятельно рекомендует устранить существующую возможность эскалации локальных привилегий посредством удаления или отключения функций LMS. Дополнительно и в качестве второго уровня защиты от случайной переустановки или включения функций LMS, настройка и выключение некоторых параметров конфигурации управления может также выполняться с помощью программ операционной системы (ОС); однако такие дополнительные локальные функции для ограничения конфигураций управления имеют недостатки последующей отмены их действия.

Примечание. Технология AMT 6.0.x не поддерживает модель локальной подготовки или управления клиентскими системами и, в результате, ее настройка не может быть отменена с помощью интерфейса ОС и приложения для обнаружения и устранения уязвимостей, INTEL-SA-00075. Для платформ, использующих встроенное ПО управления версии .0.x.x или 6.1.x.x, будет необходимо полностью отключить настройки с помощью команды ПО Intel SCS Suite, ACUConfig /full, или с помощью системного MEBx.

Для получения помощи в реализации действий устранения уязвимости, представленных в этом документе, обратитесь в [службу поддержки Intel](#). В разделе технологий выберите Intel® AMT (Intel® Active Management Technology).

Использование приложения обнаружения и устранения уязвимости, INTEL-SA-00075

Что такое приложение обнаружения и устранения уязвимости, INTEL-SA-00075?

Приложение обнаружения и устранения уязвимости (Detection and Mitigation Tool, INTEL-SA-00075), может использоваться локальными пользователями или ИТ-администратором для определения уязвимости системы к угрозам, представленным в рекомендациях Intel по безопасности, INTEL-SA-00075. Версия приложения консоли также может использоваться для выполнения действий устранения уязвимости.

Приложение обнаружения и устранения уязвимостей доступно в двух версиях.

- Первая представляет собой приложение с пользовательским интерфейсом, которое во время выполнения обнаруживает информацию об аппаратных и программных средствах устройства и сообщает оценку возможного риска. Эта версия рекомендуется, если необходима локальная оценка системы.
- Вторая версия представляет собой исполнимый модуль консоли, который выполняет оценку риска и действия для

устранения уязвимости. Кроме того, она может сохранить обнаруженную информацию в реестре Windows* и/или в файле XML. Данная версия является более удобной для ИТ-администраторов, желающих выполнять операции обнаружения и исправления сразу на нескольких компьютерах.

Загрузка приложения обнаружения и устранения уязвимостей, INTEL-SA-00075

Приложение обнаружения и устранения уязвимостей, INTEL-SA-00075, доступно в виде пакета для загрузки на сайте: <https://www.intel.com/content/www/ru/ru/support/technologies/000024133.html>.

Системные требования

- Microsoft Windows* 7, 8, 8.1 или 10
- Административный доступ к локальной операционной системе

Установка приложения

Интерактивная установка

Запустите файл INTEL-SA-00075 Detection and Mitigation Tool.msi и выполните инструкции на экране.

Автоматическая установка

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

Эта команда установит приложение обнаружения и устранения уязвимостей, INTEL-SA-00075, в каталог по умолчанию, C:\Program Files (x86)\Intel\Intel-SA-00075 Detection and Mitigation Tool\

Удаление приложения

Интерактивное удаление

Запустите файл INTEL-SA-00075 Detection and Mitigation Tool.msi и выполните инструкции на экране.

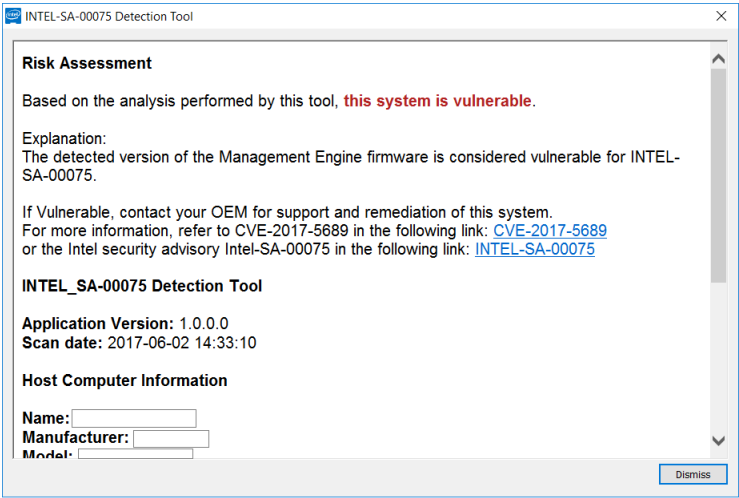
Автоматическое удаление

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

Использование приложения с пользовательским интерфейсом

Файл INTEL-SA-00075-GUI.exe предназначен для запуска на одной системе. Во время выполнения приложение отображает на экране обнаруженную информацию.

Рис. 1. Пример экрана приложения INTEL-SA-00075-GUI с выходной информацией



Использование приложения консоли

Запустите файл INTEL-SA-00075-console.exe в командной строке с административными правами.

Использование:

```
Intel-SA-00075-console.exe [[команда] | [параметр...]]
```

За один раз можно указать только одну команду. Если команда не указана, будет отображена информация обнаружения.

Таблица 1. Параметры командной строки консоли INTEL-SA-00075

Команды командной строки	Функции
-Discover	Отображает результаты на консоли и записывает данные в реестр.
-Unprovision [пароль], -u [пароль]	Удаляет все установки Intel AMT и отключает функции Intel AMT. Для устройства Intel AMT может потребоваться указать пароль администратора. ПРИМЕЧАНИЕ. Выполнение этой команды без пароля используется только с версиями встроенного ПО, работающими с приложением INTEL-SA-00075 (6.1.x.x–11.6.x.x с номером сборки менее 3000). Если используются версии встроенного ПО 6.1.x.x–11.6.x.x с номерами сборки более 3000, отмена настроек будет выполнена только с использованием пароля.
-DisableClientControlMode, -DisableCCM	Полностью выключает режим клиентского управления в устройстве Intel AMT. После выполнения этой команды устройство будет невозможно перевести в режим клиентского управления. ПРИМЕЧАНИЕ. Для отмены этого действия нет командной строки. ПРЕДУПРЕЖДЕНИЕ. Восстановление активности CCM может быть выполнено не на всех платформах.
-DisableLMS	Отключает службу LMS.

Командная строка	Функции
-n, -noregistry	Предотвращает запись результатов в реестр
-c, -noconsole	Предотвращает отображение результатов на консоли
-d, -delay <сек.>	Задержка перед запуском в секундах. Если значение не указано,

	приложение работает без задержки.
-f, -writefile	Записывает результаты в файл. Имя файла записывается в формате: <имя_компьютера>.xml
-p <путь_файла>, -filepath <путь_файла>	Путь к месту хранения файла вывода. Если путь не указан, файл будет записан в каталог запуска приложения.
-h, -help, -?	Отображает все команды, параметры и их функции

-Discover

Команда обнаружения отображает полученную информацию на консоли. По умолчанию она также записывает данные обнаружения в реестр. Если на консоли команда не указана, будет выполнено только обнаружение.

-Unprovision

Удаляет все настройки и выключает функции Intel AMT. Для устройства с технологией Intel AMT может использоваться пароль.

После конфигурации приложения Intel® AMT и ISM автоматически прослушивают трафик управления сетью вашего компьютера. В системах, имеющих известные уязвимости эскалации привилегий, настройки должны быть отключены с помощью команды отмены настроек для предотвращения несанкционированного доступа к функциям управления.

Запуск этой команды без пароля работает только с версиями встроенного ПО, представленными INTEL-SA-00075 (6.1.x.x–11.6.x.x с номерами сборки менее 3000). Если используются версии встроенного ПО 6.1.x.x–11.6.x.x с номерами сборки более 3000, отмена настроек будет выполнена только с использованием пароля.

-DisableClientControlMode

Ограничение конфигурации с использованием -DisableClientControlMode является необязательным действием для клиентов, которым необходим второй уровень защиты от уязвимостей, когда злоумышленники пытаются получить привилегии администратора ОС. Отмена этих настроек достаточно сложна и может не поддерживаться производителем компьютера, а также потребовать непосредственного доступа к системе. Если вы решили выполнить это дополнительное ограничение конфигурации, оно должно быть реализовано до отключения службы LMS.

Действия для восстановления работы CCM

Если это поддерживается производителем вашего компьютера, вы сможете выполнить сброс SKU с функциями управления Intel в системной BIOS, что вновь включит CCM. Проконсультируйтесь у производителя, чтобы узнать, поддерживается ли эта возможность и какие действия необходимы.

Примечание. Производитель может предоставить средства, позволяющие вам сконфигурировать настройки BIOS с помощью ОС. Эти средства (если доступны) могут позволить вам выполнить сброс параметров SKU с функциями управления Intel в BIOS без непосредственного физического контакта с компьютером. Обратитесь к производителю вашего компьютера, чтобы узнать о наличии средства с этой функциональностью.

-DisableLMS

Команда DisableLMS отключает службу LMS в качестве действия устранения уязвимости.

Что такое LMS?

Приложение Intel® для управления и обеспечения безопасности, LMS (Local Management Service), является службой, которая разрешает работу приложений на поддерживаемых устройствах Intel® AMT, Intel® SBA или Intel® Standard Manageability для использования обычных функций SOAP и WS-Management. Оно прослушивает порты Intel® Manageability Engine (ME) (16992, 16993, 16994, 16995, 623 и 664) и направляет трафик во встроенное ПО с помощью драйвера Intel® MEI.

Дополнительные аспекты

Любое лицо, имеющее административные привилегии в ОС, сможет переустановить службу LMS, если она удалена, или включить ее, если она выключена. Поэтому важно проявлять осторожность, чтобы избежать несанкционированной установки или включения службы LMS, пока данная уязвимость присутствует в системе. Например, службу LMS можно переустановить, если в дальнейшем вы вновь запустите установщик ПО с функциями управления Intel.

Рис. 2. Пример вывода данных на консоли INTEL-SA-00075-Console

```
Приложение обнаружения уязвимости, INTEL-SA-00075
Версия приложения: <версия приложения>
Дата сканирования: <дата и время>

*** Информация о компьютере ***
Имя компьютера: <имя компьютера>
Производитель: <производитель компьютера>
Модель: <модель компьютера>
Процессор: <модель процессора>
Версия Windows: <версия Windows*>

*** Информация ME ***
Версия: <версия встроенного ПО Intel ME>
SKU: <функция управления, если присутствует>
Состояние: <состояние подготовки ME>
Установлен драйвер: <True/False>
Режим управления: <Нет/ACM/CCM>
CCM выключено: <True/False/Неизвестно>
EHBC включено <True/False>
Состояние LMS: <активна/остановлена/отсутствует>
Тип загрузки LMS: <загрузка/система/авто/вручную/выключена/отсутствует>
Состояние MicroLMS: <активна/остановлена/отсутствует>
Тип загрузки MicroLMS: <загрузка/система/авто/вручную/выключена/отсутствует>
Наличие SPS: <True/False>

*** Оценка риска ***
На основании анализа, выполненного этим приложением,
< эта система уязвима /
эта система не имеет уязвимости /
эта система не имеет уязвимости; не Intel SKU /
эта система не имеет уязвимости; версия встроенного ПО ME не подвержена уязвимости /
эта система не имеет уязвимости; ME SKU не подвержено уязвимости /
эта система не имеет уязвимости; SMBIOS указывает на потребительский SKU /
эта система не имеет уязвимости; в системе работает встроенное ПО SPS (встроенное ПО
служб серверной платформы) /
это встроенное ПО системы было обновлено, и система находится в неподготовленном
состоянии /
это встроенное ПО системы было обновлено, и система находится в подготовленном
состоянии /
проверьте у OEM-производителя /
риск системы неизвестен>

Если система уязвима, обратитесь к OEM-производителю за поддержкой и инструкциями по
исправлению этой системы.

*** Дополнительная информация ***
См. CVE-2017-5689 на странице:
    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>

Логика, используемая для оценки риска, поясняется в Таблица 2.

Таблица 2. Значение информации оценки

Сообщение	Значение
Уязвимость	Обнаруженная версия встроенного ПО Management Engine считается уязвимой для intel-SA-00075.
Нет уязвимости	Система соответствует критерию "Нет уязвимости", описание которого представлено в <i>Идентификация уязвимости систем в помощь приложения обнаружения INTEL-SA-00075</i> на странице 8.
Встроенное ПО этой системы было обновлено, и система находится в неподготовленном состоянии	Обнаруженное встроенное ПО этой системы содержит исправление для INTEL-SA-00075. Убедитесь в том, что перед повторной подготовкой для отмены настроек системы использовалось приложение INTEL-SA-00075. Оно должно удалить любые несанкционированные настройки конфигурации.
Встроенное ПО этой системы было обновлено, и система находится в подготовленном состоянии	Обнаруженное встроенное ПО этой системы содержит исправление для INTEL-SA-00075. Если система была подготовлена до обновления встроенного ПО, процедуры полного удаления настроек и повторной подготовки позволят удалить любые несанкционированные настройки конфигурации.
Проверьте у OEM-производителя	Обнаруженная информация в SMBIOS OEM-производителя демонстрирует SKU с функциями управления, однако приложение не получило ответ после запроса подробных данных из вашего компьютера. Это может быть вызвано отсутствием драйвера интерфейса Management Engine. Обратитесь к OEM-производителю за информацией, если модель вашего компьютера находится в списке уязвимых.
Неизвестно	<p>Приложение не получило действительный ответ на запрос данных аппаратной инвентаризации вашего компьютера. Обратитесь к производителю системы за помощью в определении уязвимости этой системы.</p> <p>Это сообщение может быть получено на серверной платформе без установленного драйвера PMX. Возможно, этот драйвер доступен не для всех версий ОС Windows. Если драйвер отсутствует, рекомендуемым решением будет запуск приложений spsInfo или spsManuf, поставляемых с версией встроенного ПО SPS. Оба приложения могут использоваться для установки драйвера PMX.</p>

Результаты

Примечание. Объем данных, отображаемых командой обнаружения приложения INTEL-SA-00075, будет зависеть от наличия загруженного в системе стека драйвера с функциями управления Intel. Если драйвер интерфейса Intel® Management Engine Interface (MEI) и служба приложения управления и безопасности Intel® LMS (Local Management Service) установлены, для отображения будет доступно гораздо больше данных. Некоторые из полей могут не поддерживаться производителем системы.

Местоположение в реестре

Значения из таблицы результатов можно найти в следующем разделе реестра:

- 32-разрядные ОС: HKLM\SOFTWARE\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool
- 64-разрядные операционная системы: HKLM\SOFTWARE\WOW6432Node\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool

XML

Если вы решите записать результаты в файл XML, данный файл будет сохранен в каталоге, откуда было запущено приложение INTEL-SA-00075-console.exe, или в месте, указанном с помощью параметра командной строки. В него будет включена информация об аппаратной инвентаризации, ОС и наличии службы LMS. Если в системе присутствует поддержка AMT, в информацию также будут добавлены обнаруженные специальные хэши сертификатов. Этот список может использоваться для проверки хэшей, хранящихся в AMT.

Коды возврата консоли

Таблица 3. Коды возврата консоли INTEL-SA-00075

№	Значение
0	NOTVULNERABLE (если была запущена команда Discover) 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

Таблица 4. Выходные значения консоли INTEL-SA-00075

Значение	Расположение	Описание
Application Version (Версия приложения)		Версия используемого приложения сканирования
Scan Date (Дата сканирования)		Дата и время выполнения сканирования
Computer Name (Имя компьютера)		Имя просканированного компьютера
Computer Manufacturer (Производитель компьютера)	Аппаратная инвентаризация	Производитель компьютера
Computer Model (Модель компьютера)		Модель компьютера
Processor (Процессор)		Модель процессора компьютера
ME Version (Версия ME)	Информация о встроенном ПО ME	Строковое значение с полным номером версии встроенного ПО ME в следующем формате: Major.Minor.Hotfix.Build (основная.второстепенная.исправление.сборка)
ME SKU		Функция управления, если присутствует в системе

ME Provisioning State (Состояние подготовки ME)		Состояние конфигурации ME Не обнаружено Не подготовлено Подготовка выполняется Подготовлено
ME Driver Installed (Драйвер ME установлен)		Значение True/False, если драйвер MEI установлен на компьютере
EHBC Enabled (EHBC включено)		Значение True/False, если система может быть подготовлена с помощью конфигурации Embedded Host
LMS state (Состояние LMS)		Информация о состоянии службы LMS - активна, неактивна или отсутствует
LMS startup type (Тип запуска LMS)		Информация о типе запуска LMS - NotPresent (отсутствует), Boot (загрузка), System (системный), Auto (авто), Manuel (вручную) или Disabled (выключена)
MicroLMS state (Состояние MicroLMS)		Информация о состоянии службы MicroLMS - активна, неактивна или отсутствует
MicroLMS startup type (Тип запуска MicroLMS)		Информация о типе запуска MicroLMS - NotPresent (отсутствует), Boot (загрузка), System (системный), Auto (авто), Manuel (вручную) или Disabled (выключена)
Control Mode (Режим управления)		Режим конфигурации ME None, ACM или CCM
Is CCM Disabled (CCM выключено)		Статус True/False/Неизвестно для режима управления клиентами выключен
Is SPS (SPS)		Является ли платформа SPS (Server Platform Services) системой без уязвимости?
*** Оценка риска ***	Оценка риска	См. Таблица 2. Значение информации оценки

Идентификация уязвимости систем в помощью приложения обнаружения INTEL-SA-00075

Уязвимые системы определяются по наличию уязвимой версии встроенного ПО Intel® Management Engine (ME) и одного из трех наборов функций управления, указанных в Таблица 5.

Примечание. Платформы SPS (Server Platform Services) не являются уязвимыми по данным INTEL-SA-00075. Серверные платформы SPS имеют встроенное ПО, работающее с помощью Manageability Engine (ME) (часть PCH). Это встроенное ПО отличается от встроенного ПО с функциями управления Intel (также работает на ME) на платформах ПК/рабочих станций.

Таблица 5. Критерий определения уязвимости систем, указанных в статье INTEL-SA-00075, с помощью приложения обнаружения INTEL-SA-00075

Имя значения	Уязвимость	Нет уязвимости
ME SKU	Intel® Full AMT Manageability Intel® Standard Manageability (Стандартное управление Intel®) Преимущества для малого бизнеса Intel® (SBA)	Значения ME SKU не представлены в списке уязвимостей слева -или- Значения ME SKU слева с версией встроенного ПО, которое не имеет уязвимости
Версия ME	ME версий 6.x.x.x – 11.7.x.x со значениями сборки менее 3000 Пример: 9.5.22. 1760	Версии ME: <ul style="list-style-type: none"> 6.x.x.x – 11.7.x.x со значениями сборки более или равными 3000 <ul style="list-style-type: none"> Пример: 11.6.27.3264 2.x.x.x – 5.x.x.x 11.7.x.x или выше

Примечание. Технология Intel® Small Business (SBT) представляет собой SKU с функциями управления для технологии Преимущества для малого бизнеса Intel® (SBA).

Расширение аппаратной инвентаризации Microsoft* SCCM для добавления результатов, полученных на

консоли INTEL-SA-00075

Если вы решите хранить результаты, полученные на консоли Intel-SA-00075, в реестре Windows, вы можете использовать средство аппаратной инвентаризации Microsoft* SCCM для импорта результатов. Это позволит вам создавать коллекции в SCCM для целевых компьютеров и последующего восстановления или обновления встроенного ПО. Для этого вы должны:

1. Добавить классы аппаратной инвентаризации в файл SCCM configuration.mof.
2. Активировать эти классы аппаратной инвентаризации в вашей клиентской конфигурации.
3. Создать программный пакет для развертывания и запуска приложения консоли INTEL-SA-00075 (Intel-SA-00075-console.exe).
4. Создать последовательность задач для выполнения программного пакета.

Изменение файла MOF

Примечание. Если вы используете центральный сервер в вашем окружении, измените на нем файл MOF. Иначе сделайте эти изменения на каждом из основных серверов.

1. Найдите файл configuration.mof. Обычно он находится в папке \Program Files\Microsoft Configuration Manager\inboxex\clifiles.src\hin\
2. Сделайте резервную копию.
3. Измените файл configuration.mof, пролистав его до конца и поместите курсор над строкой:

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

4. Вставьте содержимое изменений файла MOF, представленных ранее в этом документе на странице 13-14, над строкой из третьего действия.
5. Сохраните и закройте файл.
6. Откройте приложение командной строки от имени администратора и перейдите в каталог с файлом configuration.mof.
7. Запустите приложение mofcomp без параметров, указав только файл configuration.mof.

Изменения аппаратной инвентаризации

Примечание. Для вступления в силу этих изменений необходимо время для их отправки на клиентские компьютеры и отображения новых элементов в аппаратной инвентаризации. Время вступления изменений в силу зависит от конфигурации вашего сетевого окружения.

1. Создайте новый файл с именем INTEL-SA-00075.mof.
2. Скопируйте содержимое Импорт аппаратной инвентаризации INTEL-SA-00075 на странице 165 в новый файл и сохраните его.
3. Откройте консоль диспетчера конфигураций.
4. "Администрирование > Параметры клиента > Параметры клиента по умолчанию".
5. Нажмите правой кнопкой мыши "Параметры клиента по умолчанию > Свойства".
6. Выберите "Инвентаризация оборудования > Задать классы".

7. Нажмите "Импорт".
8. Перейдите к файлу INTEL-SA-00075.mof > выберите "Открыть".
9. Убедитесь, что выбран параметр "Импортировать классы и параметры класса инвентаризации оборудования".
10. Нажмите "Импорт".
11. Нажмите "ОК > ОК".
12. SCCM запишет изменения в инвентаризацию оборудования в файле dataldr.log.

Создайте пакет SCCM

1. Создайте командный файл, представленный на странице 15, и поместите его в папку с файлом приложения консоли INTEL-SA-00075.
2. Откройте консоль диспетчера конфигураций.
3. "Библиотека ПО > Пакеты".
4. Нажмите правой кнопкой мыши "Пакеты > Создать пакет".
5. Имя: Intel-SA-00075.
6. Убедитесь, что этот пакет содержит исходные файлы.
7. Перейдите в папку пакета, указанную в первом действии.
8. Нажмите "Далее".
9. Выберите "Не создавать программу".
10. Нажмите "Далее > Далее > Заккрыть".
11. Поместите пакет в соответствующие точки распространения.

Создайте последовательность задач SCCM

1. Откройте консоль диспетчера конфигураций.
2. Перейдите "Библиотека ПО > Операционные системы".
3. Нажмите правой кнопкой мыши "Последовательности задач > Создать последовательность задач".
4. Выберите "Создать новую настраиваемую последовательность задач".
5. Нажмите "Далее".
6. Введите имя Intel-SA-00075.
7. Нажмите "Далее > Далее > Заккрыть".
8. Нажмите правой кнопкой мыши последовательность задач Intel-SA-00075 и нажмите "Изменить".
9. Перейдите "Добавить > Общие > Выполнить из командной строки".
10. Введите имя Intel-SA-00075.bat в поле командной строки.
11. Установите параметр "Пакет" и выберите "Обзор".

12. Выберите ранее созданный пакет Intel-SA-00075 > OK.
13. Нажмите "OK".

Использование приложения Intel® SCS System Discovery Utility

Что такое приложение Intel® SCS System Discovery Utility?

Приложение Intel® SCS System Discovery Utility является компонентом комплекта ПО Intel® SCS (Intel® Setup and Configuration Software), в котором содержится специальная информация об аппаратных и программных средствах в системе, поддерживающей технологию Intel® Active Management Technology (Intel® AMT), функции Intel® Standard Manageability (ISM) или технологию Intel® Small Business Technology (Intel® SBT). После запуска оно может сохранить результаты в реестре Microsoft Windows и/или файле XML. Эта информация может использоваться для выбора систем и обновления встроенного ПО или устранения уязвимостей.

Загрузка приложения Intel® SCS System Discovery Utility

Пакет загрузки приложения Intel® SCS System Discovery Utility доступен на сайте:
<https://downloadcenter.intel.com/download/26691/Intel-SCS-System-Discovery-Utility>.

Определение версии встроенного ПО управления с помощью приложения Intel® SCS System Discovery Utility

Выходные данные приложения Intel® SCS System Discovery могут использоваться для определения версии встроенного ПО системы и ее принадлежности к SKU с функциями управления. Данная информация представлена в разделе выходных данных ManageabilityInfo. Для получения инструкций по использованию приложения см. раздел *Использование приложения Intel® SCS System Discovery Utility* на стр. 12.

Значение FWVersion содержит данные о версии встроенного ПО, установленного в данный момент на устройстве. Значение AMTSKU содержит данные о поддерживаемом SKU с функциями управления, если присутствует. Проверьте значения FWVersion и AMTSKU для определения наличия уязвимости в вашей системе, как это представлено в Таблица 6.

Таблица 6. Критерий определения уязвимости, представленной в INTEL-SA-00075, с помощью приложения Intel® SCS System Discovery Utility

Имя значения	Уязвимость	Нет уязвимости
AMTSKU	Intel(R) Full AMT Manageability Intel(R) Standard Manageability Преимущества для малого бизнеса Intel(R) (SBA) Пример выходных данных: <ManageabilityInfo> <AMTSKU>Intel(R) Full AMT Manageability</AMTSKU> <AMTversion>11.0.0</AMTversion> <FWVersion>11.0.0.1202</FWVersion>	Значение AMTSKU отсутствует в выходных данных -или- Значения AMTSKU слева с версией встроенного ПО, которое не имеет уязвимости Пример выходных данных: <ManageabilityInfo> <FWVersion>9.0.13.1402</FWVersion>
FWVersion	Встроенное ПО SKU с функциями управления Intel® версий 6.x.x.x – 11.7.x.x со значением сборки менее 3000 Пример: 9.5.22. <u>1760</u>	Версии встроенного ПО SKU с функциями управления Intel®: <ul style="list-style-type: none"> • 6.x.x.x – 11.7.x.x со значениями сборки более или равными 3000 <ul style="list-style-type: none"> ○ Пример: 11.6.27.<u>3264</u> • 2.x.x.x. – 5.x.x.x • 11.7.x.x или выше

Примечание. Технология Intel® Small Business (SBT) представляет собой SKU с функциями управления для технологии Преимущества для малого бизнеса Intel® (SBA).

Использование приложения Intel® SCS System Discovery Utility

Сохранение данных только в реестре

Выполните следующую команду из командной строки с правами администратора для запуска приложения Intel® System SCS Discovery Utility и записи данных в реестр:

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

Сохранение данных только в файл XML

Используйте следующую команду для запуска приложения Intel® SCS System Discovery Utility и сохранения данных в файл XML:

```
SCSDiscovery.exe SystemDiscovery <имя файла и путь> /noregistry
```

Имя файла и путь могут быть локальными или на сетевом ресурсе. Если вы решите использовать сетевой ресурс, убедитесь в том, что учетная запись, используемая для запуска приложения Intel® SCS System Discovery Utility, имеет разрешение для записи на этом ресурсе. Если вы не укажете имя файла и путь, для файла XML будет использоваться полное доменное имя, и он будет сохранен в каталоге, содержащем приложение Intel® SCS System Discovery Utility.

Сохранение данных в реестр и файл XML

Используйте следующую команду для запуска приложения Intel® SCS System Discovery Utility и сохранения данных в реестре, и файле XML

```
SCSDiscovery.exe SystemDiscovery <имя файла и путь>
```

Как и в предыдущем примере, если вы не укажете имя файла и путь, для файла XML будет использоваться полное доменное имя, и он будет сохранен в каталоге, содержащем приложение Intel® SCS System Discovery Utility.

Результаты запуска приложения Intel® SCS System Discovery Utility

Количество данных, полученных с помощью приложения Intel® SCS System Discovery Utility, зависит от наличия загруженного в системе стека драйвера функций управления Intel. Если драйвер интерфейса Intel® Management Engine Interface (MEI) и служба приложения управления и безопасности Intel® LMS (Local Management Service) установлены, для отображения будет доступно гораздо больше данных. Представленные далее результаты предназначены для ознакомления с несколькими важными полями данных, необходимыми для устранения проблем несанкционированной эскалации привилегий. Для получения дополнительной информации о других полях данных см. документацию для приложения Intel® SCS System Discovery Utility. Некоторые из полей могут не поддерживаться производителем системы.

Результаты, сохраняемые в реестре

Сохраняемые в реестре результаты находятся в следующем местоположении:

```
HKLM\Software\Intel\Setup and Configuration Software\SystemDiscovery
```

Значения разделов:

Имя значения	Подраздел реестра	Описание значения
FWVersion	ManageabilityInfo	Версия встроенного ПО Management Engine
AMTSKU	ManageabilityInfo	Поддерживаемая функция управления, если доступна

Результаты в файле XML

Версия встроенного ПО Intel® Management Engine имеет следующий путь в файле XML:

```
<SystemDiscovery>
  <ManageabilityInfo>
    <FWVersion> Номер версии </FWVersion>
```

Поддерживаемая функция управления системой (если доступна) имеет следующий путь в файле XML:

```
<SystemDiscovery>
  <ManageabilityInfo>
    <AMTSKU> Имя функции управления </AMTSKU>
```

Импорт обнаруженных системных данных в аппаратную инвентаризацию SCCM

Процесс сбора обнаруживаемых системных данных может быть автоматизирован с помощью дополнения Intel® SCS для ПО Microsoft* System Center Configuration Manager (SCCM). После установки дополнение автоматически распространяется на аппаратную инвентаризацию SCCM для добавления обнаруженных системных данных аппаратной инвентаризации, а также создания последовательностей задач, которые могут использоваться для запуска системного обнаружения на целой коллекции систем. Накопленная во время этого процесса информация может использоваться для создания коллекций SCCM для отправки обновлений встроенного ПО или устранения уязвимостей соответствующих систем.

Пакет дополнения Intel® SCS для ПО Microsoft SCCM доступен на сайте:

<https://downloadcenter.intel.com/download/26506/Intel-SCS-Add-on-for-Microsoft-System-Center-Configuration-Manager>.

Изменения файла MOF

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

#pragma namespace ("\\\\.\\root\\cimv2")
#pragma deletelass("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 =====
```

Импорт аппаратной инвентаризации INTEL-SA-00075

```
#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;
};
```

Командный файл INTEL-SA-00075.bat

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

Примеры коллекции запросов

Подготовленные компьютеры

```
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"
```

Использование LMS

```
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"
```

ИНФОРМАЦИЯ, ПРИВЕДЕННАЯ В ЭТОМ ДОКУМЕНТЕ, ОТНОСИТСЯ К СООТВЕТСТВУЮЩЕЙ ПРОДУКЦИИ INTEL*. ЭТОТ ДОКУМЕНТ НЕ ПРЕДОСТАВЛЯЕТ НИКАКОЙ ЛИЦЕНЗИИ, ПРЯМОЙ ИЛИ КОСВЕННОЙ ДЛЯ ПРАВ НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ. ЗА ИСКЛЮЧЕНИЕМ СИТУАЦИЙ, НЕПОСРЕДСТВЕННО ОГОВОРЕННЫХ В УСЛОВИЯХ ПРОДАЖИ СООТВЕТСТВУЮЩЕЙ ПРОДУКЦИИ INTEL, КОРПОРАЦИЯ INTEL НЕ НЕСЕТ НИКАКОЙ ОТВЕТСТВЕННОСТИ И НЕ ПРЕДОСТАВЛЯЕТ ПРЯМОЙ ИЛИ КОСВЕННОЙ ГАРАНТИИ В ОТНОШЕНИИ ПРОДАЖИ И/ИЛИ ИСПОЛЬЗОВАНИЯ ПРОДУКЦИИ INTEL, В ЧАСТНОСТИ, НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ПРИГОДНОСТЬ ПРОДУКЦИИ ДЛЯ РЕШЕНИЯ КОНКРЕТНЫХ ЗАДАЧ, ОКУПАЕМОСТЬ И НЕЗАВИСИМОСТЬ ОТ ПАТЕНТОВ, АВТОРСКИХ ПРАВ ИЛИ ДРУГИХ ПРАВ НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ. ЕСЛИ ИНОЕ НЕ ПРЕДСТАВЛЕНО В ПИСЬМЕННОМ ВИДЕ КОРПОРАЦИЕЙ INTEL, ПРОДУКТЫ INTEL НЕ ПРЕДНАЗНАЧЕНЫ ДЛЯ ИСПОЛЬЗОВАНИЯ В СИСТЕМАХ, В КОТОРЫХ НЕИСПРАВНОСТЬ ПРОДУКЦИИ INTEL МОЖЕТ ПРИВЕСТИ К СИТУАЦИИ, КОТОРАЯ МОЖЕТ СТАТЬ ПРИЧИНОЙ ТРАВМ ИЛИ СМЕРТИ.

Доступность функций и преимуществ технологий Intel зависит от конфигурации системы, а для их работы может потребоваться оборудование, программное обеспечение или активация сервисов. Показатели производительности могут изменяться в зависимости от конфигурации системы. Ни одна вычислительная система не может быть полностью защищена. Проконсультируйтесь у производителя или продавца системы, или ознакомьтесь с информацией на веб-сайте intel.com.

© Корпорация Intel, 2017 г. Все права защищены. Intel и логотип Intel являются товарными знаками корпорации Intel в США и/или других странах.

* Другие наименования и товарные знаки являются собственностью своих законных владельцев.