INTEL-SA-00075 Guía de herramientas detección y mitigación

Tecnología de administración activa Intel® (Intel® AMT), Intel® Standard Manageability (Intel® ISM) y Tecnología Intel® para pequeñas empresas (Intel® SBT)

Instrucciones para detectar y mitigar INTEL-SA-00075

Revisión 1.1 – 20 de julio de 2017

Introducción

Este documento lo guiará a través de varios procesos para detectar y mitigar la vulnerabilidad de seguridad que se describe en INTEL-SA-00075. Lea el público Aviso de seguridad público en https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr para obtener más información.

Si usted es usuario de una sola PC y desea determinar su estado: Le ofrecemos la aplicación GUI de detección de INTEL-SA-00075 (Intel-SA-00075-gui.exe) para realizar un análisis local de un sistema único o independiente.

Si desea determinar el estado o aplicar mitigaciones para varias máquinas: Hemos proporcionado la aplicación (Intel-SA-00075-console.exe) de consola de la Herramienta de detección y mitigación INTEL-SA-00075. Esta herramienta puede realizar el descubrimiento y escribir sus hallazgos en el registro de Windows local y (opcionalmente) en un archivo XML, para su subsiguiente recopilación y análisis. La aplicación de consola también puede ayudar a implementar mitigaciones. Consulte *Uso de la Herramienta de detección y* mitigación INTEL-SA-00075 en la página 2 para obtener más información.

Si usted es un administrador de red que ya está usando Intel® Setup and Configuration Software (Intel® SCS): La suite Intel® SCS contiene una herramienta de consola alternativa, la utilidad Intel® SCS System Discovery. Le sugerimos el uso de esta herramienta, si ya está familiarizado con las herramientas de Intel® SCS o si desea obtener información detallada acerca de Intel® AMT. Consulte *Uso de Intel® SCS Discovery Utility* en la página 111.

Mitigación

Los pasos de mitigación descritos en este documento están destinados a evitar la activación y el uso no autorizados de los SKU de administración de Intel, la tecnología de administración activa Intel® (Intel® AMT), Intel® Standard Manageability (ISM) y la Tecnología Intel® para pequeñas empresas (Intel® SBT), que no han aplicado la actualización del firmware para resolver la vulnerabilidad.

Los profesionales de TI pueden utilizar estas instrucciones como base para las tareas o comandos dentro de las consolas de administración para implementaciones a gran escala de los pasos de mitigación. Los pasos de procedimiento para la implementación de la mitigación son los siguientes:

1. Eliminar el abastecimiento de clientes de SKU de administración de Intel para mitigar la posibilidad de que un atacante de la red acceda a los privilegios del sistema
2. Deshabilitar o eliminar el Servicio de administración local (LMS) para mitigar la posibilidad de que un atacante local sin privilegios acceda a los privilegios del sistema
3. Configurar opcionalmente las restricciones de configuración de administración local

Intel recomienda encarecidamente que el primer paso en todas las vías de mitigación sea eliminar el abastecimiento de los SKU de administración de Intel para resolver la vulnerabilidad de escalamiento de privilegios de red. Para los sistemas abastecidos, la anulación del abastecimiento debe realizarse antes de deshabilitar o eliminar el LMS. Hasta que se disponga del firmware actualizado de los SKU de administración de Intel, Intel recomienda encarecidamente mitigar la escalada de privilegios locales mediante la eliminación o desactivación del LMS. Opcionalmente, como un segundo nivel de defensa contra una reinstalación o rehabilitación inadvertida del LMS, algunas de las opciones de configuración de administración realizadas a través del sistema operativo además se pueden deshabilitar por medio del sistema operativo (SO). Sin embargo, estas restricciones adicionales a la configuración de administración local tienen limitaciones en cuanto a la forma en que se permite su reversión.

Nota: AMT 6.0.*x* no es compatible con el modelo de Control de abastecimiento/cliente base de host, y en consecuencia no puede desabastecerse mediante la interfaz del sistema operativo local a través de la Herramienta de detección y mitigación INTEL-SA-00075. Para las plataformas que utilizan Manageability Firmware 6.0.*x.x* o 6.1.*x.x*, será necesario anular totalmente abastecimiento utilizando ACUConfig /full de Intel SCS Suite o por medio de los MEBx del sistema.

Para obtener ayuda para la implementación de los pasos de mitigación proporcionados en este documento, póngase en contacto con Asistencia al cliente de Intel; en la sección Tecnologías, seleccione Tecnología de administración activa Intel® (Intel® AMT).

Uso de la Herramienta de detección y mitigación INTEL-SA-00075

¿Qué es la Herramienta de detección y mitigación INTEL-SA-00075?

La Herramienta de detección y mitigación INTEL-SA-00075 pueden ser utilizada por los usuarios locales o administradores de TI para determinar si un sistema es vulnerable a la vulnerabilidad documentada en la Advertencia de seguridad de Intel INTEL-SA-00075. La versión de la consola de la herramienta puede utilizarse para llevar a cabo los pasos de mitigación.

La Herramienta de detección y mitigación se ofrece en dos versiones.

- La primera es una herramienta interactiva de interfaz gráfica de usuario que, cuando se ejecuta, descubre los detalles de hardware y software del dispositivo y proporciona una indicación de la evaluación de riesgos. Esta versión es recomendable cuando se desea realizar una evaluación local del sistema.
- La segunda versión es una consola ejecutable que puede realizar la evaluación de riesgos y los pasos de mitigación recomendados. Opcionalmente, puede guardar la información de descubrimiento en el registro de Windows* y/o en un archivo XML. Esta versión es más conveniente para los administradores de TI que desean realizar las operaciones de descubrimiento y mitigación en grandes cantidades a través de múltiples máquinas.

Obtención de la Herramienta de detección y mitigación INTEL-SA-00075

El paquete de descarga de la Herramienta de detección y mitigación INTEL-SA-00075 está disponible en: https://www.intel.com/content/www/xl/es/support/technologies/000024133.html.

Requisitos del sistema

- Microsoft Windows* 7, 8, 8.1 o 10
- Acceso administrativo al sistema operativo local

Cómo instalar la herramienta

Instalación interactiva

Ejecute INTEL-SA-00075 Detection and Mitigation Tool.msi y siga las indicaciones en la pantalla.

Instalación silenciosa

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

Esto instalará la Herramienta de detección y mitigación INTEL-SA-00075 en el directorio predeterminado, `C:\Program Files (x86)\Intel\Intel-SA-00075 Detection and Mitigation Tool\`

Desinstalación de la herramienta

Desinstalación interactiva

Ejecute INTEL-SA-00075 Detection and Mitigation Tool.msi y siga las indicaciones en la pantalla.

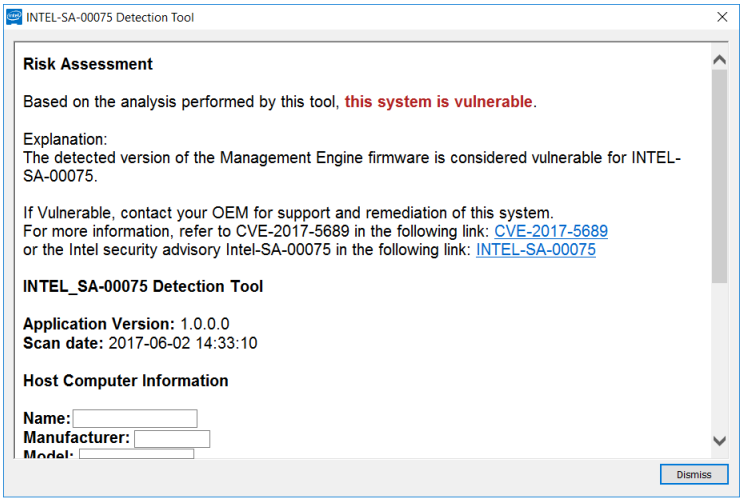
Desinstalación silenciosa

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

Ejecute la herramienta interfaz gráfica de usuario

INTEL-SA-00075-GUI.exe ha sido diseñado para ejecutarse en un solo sistema. Cuando se ejecuta, la herramienta vuelca la información de descubrimiento a la pantalla.

Figura 1. Ejemplo de la pantalla de resultados de INTEL-SA-00075-GUI



Ejecución de la herramienta de consola

Ejecute `INTEL-SA-00075-console.exe` desde un indicador de comandos con derechos de administración.

Uso:

```
Intel-SA-00075-console.exe [[command] | [option...]]
```

Solo se puede ejecutar un comando por vez. Si no se proporciona ningún comando, se ejecuta el comando "discover".

Tabla 1. Conmutadores de línea de comandos de consola INTEL-SA-00075

Comando de línea de comandos	**Funciones**
-Discover	Vuelca los resultados en la consola de salida y escribe los datos en el registro.
-Unprovision [password], -u [password]	Elimina todas las configuraciones de Intel AMT y desactiva las características de Intel AMT; se puede utilizar y podría requerirse una contraseña de usuario administrador para el dispositivo Intel AMT. NOTA: Invocar este comando sin una contraseña funciona solamente con versiones de firmware afectadas por INTEL-SA-00075 (6.1.*x.x*–11.6.*x.x* con un número de versión inferior a 3000). Si se utilizan las versiones de firmware 6.1.x.*x*–11.6.*x.x* con un número de versión superior a 3000, el desabastecimiento sólo funcionará si se proporciona una contraseña.
-DisableClientControlMode, -DisableCCM	Deshabilita de forma permanente la opción de modo Control del cliente en el dispositivo Intel AMT. Después de ejecutar este comando, el dispositivo no puede ponerse en modo Control de cliente. NOTA: No hay ningún comando CLI para revertir esta acción. ADVERTENCIA: No todas las plataformas pueden volver a activar CCM una vez desactivado.
-DisableLMS	Desactiva el servicio LMS.

Opción de línea de comandos	**Funciones**
-n, -noregistry	Impide la escritura de los resultados en el registro
-c, -noconsole	Impide que los resultados se muestran en la consola
-d, -delay <seconds>	Demora en segundos antes de que comience la ejecución. Si no se especifica ningún valor, la herramienta no experimentará ninguna demora.
-f, -writefile	Especifica los resultados de la escritura en un archivo. El nombre del archivo utiliza el siguiente formato: <computername>.xml
-p <filepath>, -filepath <filepath>	La ruta para almacenar el archivo de salida. Si no se especifica ninguna ruta, el archivo se escribirá en el directorio que está en ejecución de la herramienta.
-h, -help, -?	Muestra estos conmutadores de línea de comandos y sus funciones

-Discover

El comando "discover" vuelva la información de descubrimiento en la consola. De forma predeterminada, también escribe los datos de descubrimiento en el registro. Si no se envía ningún comando a la herramienta de consola, se ejecuta el comando "discover".

-Unprovision

Elimina todas las configuraciones de Intel AMT y desactiva las características de Intel AMT; puede usarse una contraseña de usuario administrador opcional para el dispositivo Intel AMT.

Cuando están configuradas, las tecnologías Intel® AMT e ISM automáticamente escuchan el tráfico de administración a través de la red del equipo. Los sistemas que son vulnerables al problema conocido de escalamiento de privilegios deben ser desabastecidos mediante el uso del comando "unprovision" para evitar el acceso no autorizado a las características de administración.

Invocar este comando sin una contraseña funciona solamente con versiones de firmware afectadas por INTEL-SA-00075 (6.1.*x.x*–11.6.*x.x* con un número de versión inferior a 3000). Si se utilizan las versiones de firmware 6.1.x.*x*–11.6.*x.x* con un número de versión superior a 3000, el desabastecimiento sólo funcionará si se proporciona una contraseña.

-DisableClientControlMode

La restricción de configuración -DisableClientControlMode es un paso opcional para los clientes que requieren un nivel secundario para protegerse contra la reversión de mitigación por parte de un atacante sin privilegios que obtiene acceso a privilegios de administrador del sistema operativo. Revertir estas opciones es difícil, podría no ser admitido por el fabricante del equipo y podría requerir acceso físico al sistema. Si decide realizar esta restricción de configuración adicional, se la debe realizar antes de deshabilitar el servicio LMS.

Pasos para volver a activar CCM

Si el fabricante lo admite, usted podría restablecer el SKU de administración de Intel desde el BIOS, lo que reactivaría el CCM. Consulte con el fabricante para ver si admite esta capacidad y para ver los pasos a seguir.

Nota: El fabricante podría proporcionar herramientas que le permitan configurar el BIOS a través del sistema operativo. Estas herramientas, si están disponibles, podrían permitirle restablecer los SKU de administración de Intel en el BIOS sin tener que tocar físicamente el equipo. Consulte con el fabricante para ver si ofrece una herramienta con esta funcionalidad.

-DisableLMS

El comando "DisableLMS" deshabilita el servicio LMS como un paso de mitigación.

¿Qué es LMS?

Intel® Management and Security Application Local Management Service (LMS) es un servicio que permite que las aplicaciones que se ejecutan en dispositivos compatibles con Intel® AMT, Intel® SBA o Intel® Standard Manageability utilicen funciones de SOAP y de WS-Management comunes. Escucha los puertos de Intel® Manageability Engine (ME) (16992, 16993, 16994, 16995, 623 y 664) y direcciona el tráfico al firmware a través del controlador Intel® MEI.

Consideraciones adicionales

Cualquier persona con privilegios administrativos para el sistema operativo podrá volver a instalar el LMS, si se lo elimina, o volver a activar el servicio si está deshabilitado. Por lo tanto, es importante tener cuidado para evitar una reinstalación o reactivación involuntaria del LMS, mientras exista la vulnerabilidad en el sistema. Por ejemplo, se podría volver a instalar el LMS si ejecuta el instalador de software de administración de Intel en algún momento en el futuro.

Figura 2. Ejemplo de resultados de INTEL-SA-00075-Console

```
Herramienta de descubrimiento INTEL-SA-00075
Versión de la aplicación: <versión de la aplicación>
Fecha de escaneo: <fecha y hora>

***Información del equipo host ***
Nombre del equipo: <nombre del equipo>
Fabricante: <fabricante del equipo>
Modelo: <modelo del equipo>
Procesador: <modelo del procesador>
Versión de Windows: <versión de Windows*>

*** Información de ME ***
Versión: <versión de firmware ME de Intel >
```

```
SKU: <característica de administración, si la hay>
Estado: <Estado de abastecimiento de ME >
Controlador instalado: <verdadero/falso>
Modo de control: <Ninguno/ACM/CCM>
CCM ha sido desactivado: <verdadero/falso/desconocido>
EHBC habilitado <verdadero/falso>
Estado LMS: <ejecución/detenido/no se encuentra>
Tipo de inicio LMS: <inicio/sistema/automático/manual/deshabilitado/no se encuentra>
Estado de MicroLMS: <ejecución/detenido/no se encuentra>
Tipo de inicio MicroLMS: <inicio/sistema/automático/manual/deshabilitado/no se
encuentra>
Es SPS: <verdadero o falso>


***Evaluación de riesgos***
Según el análisis realizado por esta herramienta,
< este sistema es vulnerable /
este sistema no es vulnerable /
este sistema no es vulnerable; SKU que no es Intel /
este sistema no es vulnerable; la versión de FW ME no ha sido afectada /
este sistema no es vulnerable; el SKU de ME no ha sido afectado /
este sistema no es vulnerable; el SMBIOS indica que se trata de SKU para
consumidores /
este sistema no es vulnerable; el sistema está ejecutando SPS FW (Firmware de
servicios de plataforma de servidor) /
se ha actualizado el Firmware del sistema y el sistema está en estado desabastecido
/
se ha actualizado el Firmware del sistema, y el sistema está en estado abastecido /
Consultar al OEM /
no se conoce el riesgo del sistema>

Si está Vulnerable, póngase en contacto con el OEM para obtener asistencia y
reparaciones para el sistema.

***Para obtener más información***
Consulte CVE-2017-5689 en:
     https://nvd.nist.gov/vuln/detail/CVE-2017-5689

o el Aviso de seguridad de Intel Intel-SA-00075 en:
     https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-
00075&languageid=en-fr
```

La lógica que se utiliza para determinar una evaluación de riesgos se describe en Tabla 2.

Tabla 2. Significado de la evaluación de riesgos en los resultados

Mensaje	Significado
Vulnerable	La versión del firmware del motor de administración detectada se considera vulnerable para INTEL-SA-00075.
No vulnerable	El sistema cumple con los criterios de "No vulnerable" descritos en *Identificación de sistemas afectados con la Herramienta de* descubrimiento INTEL-SA-00075 en la página 8.
Se ha actualizado el Firmware del sistema y el sistema está en estado de desabastecimiento	El firmware detectado en este sistema cuenta con la solución de INTEL-SA-00075. Asegúrese de que se utilizaron las herramientas de INTEL-SA-00075 para llevar a cabo un desabastecimiento completo del sistema antes de reabastecimiento. Esto eliminará cualquier configuración no autorizada.

Mensaje	Significado
Se ha actualizado el Firmware del sistema, y el sistema está en estado abastecido	El firmware detectado en este sistema cuenta con la solución de INTEL-SA-00075. Si el sistema fue abastecido antes de la actualización del firmware, un desabastecimiento completo y reabastecimiento del sistema eliminará cualquier configuración no autorizada.
Solicite información al OEM.	La información detectada en el SMBIOS del OEM muestra un SKU de administración, pero la herramienta no ha recibido una respuesta al solicitar información detallada de su equipo. Esto puede deberse a la ausencia de un controlador de interfaz de motor de administración. Consulte al OEM para averiguar si el modelo del equipo ha sido afectado.
Desconocido	La herramienta no ha recibido una respuesta válida al solicitar los datos de inventario de hardware de su equipo. Póngase en contacto con el fabricante del sistema para recibir ayuda y determinar la vulnerabilidad de este sistema. Puede recibir este mensaje en una plataforma de servidor sin tener instalado un controlador PMX. Este controlador podría no estar disponible en todas las versiones del sistema operativo Windows. Si el controlador no está presente, la solución recomendada es ejecutar la aplicación spsInfo o spsManuf proporcionada con la versión de Firmware SPS. Ambas aplicaciones instalarán al controlador de PMX.

Resultado

Nota: La cantidad de datos devueltos por el comando "Discover" de INTEL-SA-00075 dependerá de si la pila de controlador de administración de Intel está cargado en el sistema. Si el controlador de la Interfaz del motor de administración Intel® (MEI) e Intel® Management and Security Application Local Management Service (LMS) están presentes, habrá un conjunto más detallado de datos disponible. Algunos de los campos podrían no ser admitidos por el fabricante.

Ubicación del registro

Los valores de la tabla de resultados pueden encontrarse en la clave de registro siguiente:

- Sistemas operativos de 32 bits:`HKLM\SOFTWARE\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool`
- Sistemas operativos de 64 bits: `HKLM\SOFTWARE\WOW6432Node\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool`

XML

Si decide escribir los resultados en un archivo XML, ese archivo se almacenará en el directorio desde el cual se ejecuta INTEL-SA-00075-console.exe o en la ruta especificada en las opciones de línea de comandos. Se incluye información como inventario de hardware, sistema operativo, presencia LMS. Si está AMT está presente se incluirá la lista de hashes certificados personalizados y predeterminados. Esta lista puede utilizarse para auditar hashes esperados en comparación con lo que se almacena en AMT.

Códigos de retorno de la consola

Tabla 3. Códigos de retorno de la consola INTEL-SA-00075

Número	Significado

Número	Significado
0	NOTVULNERABLE (si se ejecutó el comando "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

Tabla 4. Valores de resultado de la consola INTEL-SA-00075

Valor	Ubicación	Descripción
Application Version (Versión de la aplicación)		La versión de la herramienta de escaneo utilizada
Scan Date (Fecha de escaneo)		La fecha y la hora en que se realizó el escaneo
Computer Name (Nombre de computadora)		El nombre del equipo escaneado
Computer Manufacturer (Fabricante del equipo)	Inventario de hardware	El fabricante del equipo
Computer Model (Modelo del equipo)		El modelo del equipo
Processor (Procesador)		Modelo del procesador de la computadora
ME Version (Versión de ME)	Información del firmware de ME	Una valor de cadena con el número de la versión de firmware de ME completo con el formato siguiente: Major.Minor.Hotfix.Build
ME SKU (SKU de ME)		Si existe; si se cuenta con administración en el sistema
ME Provisioning State (Estado de abastecimiento de ME)		El estado de configuración de ME No se ha detectado ninguno No abastecido En proceso de abastecimiento Abastecido
ME Driver Installed (Controlador de ME instalado)		Valor de verdadero o falso si el controlador MEI está presente en el equipo
EHBC Enabled (EHBC activado)		Valor de verdadero o falso si el sistema es apto para el método de abastecimiento de Configuración basada en host integrado
LMS state (Estado de LMS)		Información sobre si se está ejecutando el servicio LMS, no se lo está ejecutando o no está presente
LMS startup type (Tipo de inicio de LMS)		Información sobre si el tipo de inicio de LMS es No se encuentra, inicio, sistema, automático, manual o desactivado
MicroLMS state (Estado de MicroLMS)		Información sobre si se está ejecutando el servicio MicroLMS, no se lo está ejecutando o no está presente
MicroLMS startup type (Tipo de inicio de MicroLMS)		Información sobre si el tipo de inicio de MicroLMS es No se encuentra, inicio, sistema, automático, manual o desactivado
Control Mode (Modo de control)		El modo de configuración de ME Ninguno, ACM o CCM
Is CCM Disabled (CCM desactivado)		Estado Verdadero/Falso/Desconocido en cuanto a si el Modo de control del cliente está desactivado
Is SPS (¿Es SPS?)		¿Es la plataforma un sistema de Servicios de plataforma de servidor (SPS) no vulnerable?

Evaluación de riesgos	Evaluación de riesgos	Consulte *Tabla 2. Significado de la evaluación de riesgos en los resultados*

Identificación de sistemas afectados con la Herramienta de descubrimiento INTEL-SA-00075

Los sistemas afectados se definen como aquellos que tienen una versión de firmware de Intel® Management Engine (ME) que contiene uno de los tres conjuntos de características de capacidad de administración que se definen en Tabla 5.

Nota: Las plataformas de Servicios de plataforma de servidor (SPS) no son vulnerables a INTEL-SA-00075. Las plataformas SPS tienen firmware que se ejecuta en el motor de administración (ME) (parte de PCH) en las plataformas de servidor. Este firmware es diferente al firmware de administración Intel (que también se ejecuta en ME) en las plataformas de PC y estaciones de trabajo.

Tabla 5. Criterios para determinar si un sistema es vulnerable a INTEL-SA-00075 utilizando la Herramienta de descubrimiento INTEL-SA-00075

Nombre del valor	Vulnerable	No vulnerable
`SKU de ME`	Intel® Full AMT Manageability Función Intel® de administración estándar Ventaja Intel® para pequeñas empresas (SBA)	No hay valores de SKU ME presentes en la lista de vulnerabilidad a la izquierda o Los valores de SKU ME a la izquierda tienen una versión de firmware que no es vulnerable
`Versión de ME`	Versiones de ME 6.x.x.x – 11.7.x.x con un valor de versión menor que 3000 Ejemplo: 9.5.22.**1760**	Versiones de ME: • 6.x.x.x – 11.7.x.x con un valor de versión igual a o mayor que 3000 ○ Ejemplo: 11.6.27.**3264** • 2.x.x.x. – 5.x.x.x • 11.7.x.x o superior

Nota: La Tecnología Intel® para pequeñas empresas (SBT) es el SKU de administración de Intel® Small Business Advantage (SBA).

Ampliación de inventario del hardware Microsoft * SCCM para incluir los resultados de la herramienta de consola INTEL-SA-00075

Si decide almacenar los resultados de la herramienta de consola de Intel-SA-00075 en el registro de Windows, puede aprovechar la capacidad de ampliación de inventario de hardware de Microsoft* SCCM para importar los resultados. Esto le permitirá sumar colecciones de SCCM para equipos de destino con el fin de reparar o actualizar el firmware. Para ello, tendrá que hacer lo siguiente:

1. Agregar clases de inventario de hardware en el archivo configuration.mof de SCCM.
2. Habilitar estas nuevas clases de inventario de hardware en la configuración del cliente.
3. Crear un paquete de software para implementar y ejecutar la herramienta de consola de INTEL-SA-00075 (`console.exe-Intel-SA-00075)`.
4. Crear una secuencia de tareas para ejecutar el paquete de software.

Modificar los archivos MOF

Nota: Si tiene un servidor central en su entorno, modifique el archivo MOF en ella. De lo contrario, realice estos cambios en cada uno de los servidores principales.

1. Busque el archivo configuration.mof. Por lo general se encuentra en \Program Files\Microsoft Configuration Manager\inboxex\clifiles.src\hinv\
2. Realice una copia de seguridad.
3. Edite el archivo configuration.mof, desplazándose hasta el final de la ubicación del archivo y colocando el cursor por encima de esta línea:

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

4. En este documento antes de la línea del paso tres, pegue el contenido de los cambios en el archivo MOF de las páginas 13 y 14.
5. Guarde y cierre el archivo.
6. Inicie un indicador de comandos que se ejecute como administrador en el directorio con configuration.mof.
7. Ejecute mofcomp sin conmutadores destinados al archivo configuration.mof modificado.

Cambios en el inventario de hardware

Nota: Una vez realizados, estos cambios necesitan tiempo para propagarse a los clientes antes de que aparezcan los nuevos elementos en el inventario de hardware. La cantidad de tiempo que lleve pueden variar dependiendo de cómo esté configurado su entorno.

1. Cree un nuevo archivo denominado INTEL-SA-00075.mof.
2. Pegue el contenido de Importación de inventario de hardware de INTEL-SA-00075 en la página 165 en el archivo recientemente creado y guárdelo.
3. Inicie la Consola de administración de configuración.
4. Administración > Configuración de cliente > Configuración de cliente predeterminado.
5. Haga clic derecho en la Configuración de cliente predeterminada > Propiedades.
6. Seleccione Inventario de hardware > Establecer clases.
7. Haga clic en Importar.
8. Navegue hasta el archivo INTEL-SA-00075.mof > Abrir.
9. Compruebe que esté seleccionada la opción "Importar las clases de inventario de hardware y configuración de clase de inventario de hardware".
10. Haga clic en Importar.
11. Aceptar > Aceptar.
12. SCCM registra los cambios en el Inventario de hardware en el archivo dataldr.log.

Crear paquete SCCM

1. Cree el archivo por lotes de la página 15 y colóquelo en una carpeta con el archivo de herramienta de consola INTEL-SA-00075.
2. Inicie la Consola de administración de configuración.
3. Biblioteca de software > Paquetes.
4. Haga clic derecho en Paquetes > Crear paquete.

5. Nombre: Intel-SA-00075
6. Verifique si este paquete contiene archivos de origen.
7. Navegue hasta la carpeta del paquete del paso uno.
8. Siguiente.
9. Seleccione No crear un programa.
10. Siguiente > Siguiente > Cerrar.
11. Distribuya el paquete a los Puntos de distribución apropiados.

Crear secuencia de tarea SCCM

1. Inicie la Consola de administración de configuración.
2. Biblioteca de software > Sistemas operativos.
3. Haga clic derecho en las secuencias de tareas > Crear secuencia de tareas.
4. Seleccione Crear una nueva secuencia de tareas personalizada.
5. Siguiente.
6. Escriba un nombre de Intel-SA-00075.
7. Siguiente > Siguiente > Cerrar.
8. Haga clic derecho en la secuencia de tareas de Intel-SA-00075 haga clic en Editar.
9. Agregar > General > Ejecutar línea de comandos.
10. Ingrese Intel-SA-00075.bat en el campo Línea de comandos.
11. Marque la casilla Paquete y seleccione Examinar.
12. Seleccione el paquete Intel-SA-00075 creado anteriormente > Aceptar.
13. Haga clic en Aceptar.

Uso de Intel® SCS Discovery Utility

¿Qué es Intel® SCS System Discovery Utility?

Intel® SCS System Discovery Utility es un componente de Intel® Setup and Configuration Software (Intel® SCS) que le proporcionará detalles específicos del hardware y software en un sistema que sea compatible con la Tecnología de administración activa Intel® (Intel® AMT), Intel® Standard Manageability (ISM) o la Tecnología Intel® para pequeñas empresas (Intel® SBT). Cuando se ejecuta, puede guardar los resultados en el registro de Microsoft Windows y/o en un archivo XML. Esta información puede utilizarse para encontrar los sistemas de destino para actualizar el firmware o para implementar mitigaciones.

Cómo obtener el sistema de Intel® SCS System Discovery Utility

El paquete de descarga de Intel® SCS System Discovery Utility está disponible en https://downloadcenter.intel.com/download/26691/Intel-SCS-System-Discovery-Utility.

Determinar la versión de firmware de administración utilizando Intel® SCS System Discovery Utility

El resultado de Intel® SCS System Discovery Utility se puede utilizar para determinar la versión del firmware de un sistema y si el sistema es un SKU de administración. Esta información se proporciona en la sección `ManageabilityInfo` de los resultados. Para obtener instrucciones sobre cómo ejecutar la herramienta, tenga a bien leer la sección *Ejecutar Intel® SCS System Discovery Utility* en la página 12.

El valor de `FWVersion` contiene la versión del firmware actualmente en el dispositivo. El valor `AMTSSKU` contiene el SKU de administración compatible, si lo hay. Revise los valores de `FWVersion` y `AMTSKU` para determinar las vulnerabilidades de su sistema tal como se describe en Tabla 6.

Tabla 6. Criterios para determinar si un sistema es vulnerable a INTEL-SA-00075 utilizando Intel® SCS System Discovery Utility

Nombre del valor	Vulnerable	No vulnerable
`AMTSKU`	Intel(R) Full AMT Manageability Intel(R) Standard Manageability Intel(R) Small Business Advantage(SBA) Ejemplo de resultados: <ManageabilityInfo> <AMTSKU>**Intel(R) Full AMT Manageability**</AMTSKU> <AMTversion>**11.0.0**</AMTversion> <FWVersion>**11.0.0.1202**</FWVersion>	El valor AMTSKU no está presente en los resultados o Valores AMTSKU a la izquierda con una versión de firmware que no es vulnerable Ejemplo de resultados: <ManageabilityInfo> <FWVersion>**9.0.13.1402**</FWVersion>
`FWVersion`	Versiones de firmware del SKU de administración Intel® 6.x.x.x – 11.7.x.x con un valor de versión inferior a 3000 Ejemplo: 9.5.22.**1760**	Versiones de firmware de SKU administración Intel®: • 6.x.x.x – 11.7.x.x con un valor de versión igual a o mayor que 3000 o Ejemplo: 11.6.27.**3264** • 2.x.x.x. – 5.x.x.x • 11.7.x.x o superior

Nota: La Tecnología Intel® para pequeñas empresas (SBT) es el SKU de administración de Intel® Small Business Advantage (SBA).

Ejecución de Intel® SCS System Discovery Utility

Guardar datos en el registro solamente

Ejecute el siguiente comando desde un indicador de comandos con derechos de administrador para ejecutar Intel® System SCS Discovery Utility y escribir datos en el registro:

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

Guardar los datos en un archivo XML solamente

Utilice el siguiente comando para ejecutar Intel® SCS System Discovery Utility y guardar los datos en un archivo XML:

```
SCSDiscovery.exe SystemDiscovery <nombre de archivo y ruta> /noregistry
```

El nombre del archivo y la ruta de acceso pueden ser una ubicación local en el sistema o un recurso compartido de red. Si decide utilizar un recurso compartido de red, asegúrese de que la cuenta que ejecute Intel® SCS System Discovery Utility tenga los permisos de escritura para ese recurso compartido de red. Si no especifica un nombre de archivo y una ruta, se utilizará el FQDN del sistema para el nombre del archivo XML y el archivo se almacenará en el directorio que contiene Intel® SCS System Discovery Utility.

Guardar los datos en el registro y en un archivo XML

Utilice el siguiente comando para ejecutar Intel® SCS System Discovery Utility y guardar datos en el registro y en un archivo XML

```
SCSDiscovery.exe SystemDiscovery <nombre de archivo y ruta>
```

Como en el ejemplo anterior, si no especifica un nombre de archivo y una ruta, se utilizará el FQDN del sistema para el nombre del archivo XML y el archivo se almacenará en el directorio que contiene Intel® SCS System Discovery Utility.

Resultados de Intel® SCS System Discovery Utility

La cantidad de datos generados por Intel® SCS System Discovery Utility dependerá de si la pila de controladores de administración de Intel está cargada en el sistema. Si el controlador de la Interfaz del motor de administración Intel® (MEI) e Intel® Management and Security Application Local Management Service (LMS) están presentes, habrá un conjunto más detallado de datos disponible. Los resultados que se describen a continuación se centrarán en tan solo algunos campos de datos clave relevantes para el problema de escalamiento de privilegios conocido. Para obtener más información sobre los otros campos de datos, consulte la documentación de Intel® SCS System Discovery Utility. Algunos de los campos podrían no ser admitidos por el fabricante.

Resultados del registro

Los resultados que se guardan en el registro pueden encontrarse en la ubicación siguiente:
`HKLM\Software\Intel\Setup and Configuration Software\SystemDiscovery`

Valores clave:

Nombre del valor	Clave de subregistro	Descripción del valor
FWVersion	ManageabilityInfo	Versión de firmware de Intel® Management Engine
AMTSKU	ManageabilityInfo	Función de administración compatible, si la hay

Resultados del archivo XML

La versión de firmware de Intel® Management Engine se encuentra en la siguiente ruta en el archivo XML:

```
<SystemDiscovery>
       <ManageabilityInfo>
              <FWVersion> Número de versión </FWVersion>
```

La función de administración compatible del sistema, si la hay; se encuentra en la siguiente ruta en el archivo XML:

```
<SystemDiscovery>
       <ManageabilityInfo>
              <AMTSKU> Nombre de la función de administración </AMTSKU>
```

Importar datos de descubrimiento del sistema al inventario de hardware SCCM

El proceso de recopilación de datos de descubrimiento del sistema puede automatizarse con el complemento de Intel® SCS para Microsoft* System Center Configuration Manager (SCCM). Una vez instalado, este complemento ampliará automáticamente el inventario de hardware SCCM incluyendo los datos de descubrimiento del sistema, y también creará secuencias de tareas que se pueden utilizar para ejecutar el descubrimiento de sistemas en función de colecciones de sistemas. La información recopilada a través de este proceso, a continuación, puede utilizarse para crear colecciones de SCCM para realizar actualizaciones de firmware o mitigaciones en sistemas afectados.

El paquete de descarga del complemento Intel® SCS para Microsoft SCCM está disponible en https://downloadcenter.intel.com/download/26506/Intel-SCS-Add-on-for-Microsoft-System-Center-Configuration-Manager.

Cambios en los archivos MOF

```
//======= 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 ====
```

Importación de inventario de hardware de 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;
};
```

Archivo de lote 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 /IMPLEVEL:Impersonate /AUTHLEVEL:Pktprivacy /namespace:\\root\ccm path sms_client CALL
TriggerSchedule %HWInventoryGUID% /NOINTERACTIVE
echo Exit code: %EL%
exit %EL%
```

Ejemplos de consultas de recopilación

Equiposabastecidos

```
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"
```

Ejecución de 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"
```