Guia da Ferramenta de detecção e minimização INTEL-SA-00075

Intel® Active Management Technology (Intel® AMT) Intel® Standard Manageability (ISM) e Tecnologia Intel® para pequenas empresas (SBT)

Instruções para detectar e minimizar INTEL-SA-00075
Revisão 1.1 — 20 de julho de 2017

Introdução

Este documento o orientará ao longo dos vários processos para detectar e minimizar a vulnerabilidade da segurança, descrita na INTEL-SA-00075. Leia o Alerta sobre segurança pública, em https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr para obter mais informações.

Para o usuário de um PC individual, que deseja determinar o status do equipamento: fornecemos o aplicativo da GUI de detecção INTEL-SA-00075 (Intel-SA-00075-gui.exe) para análise local de um sistema individual ou independente.

Para determinar o status e/ou aplicar minimizações a várias máquinas: fornecemos o aplicativo de console da Ferramenta de detecção e minimização INTEL-SA-00075 (Intel-SA-00075-console.exe). Essa ferramenta pode executar a descoberta e gravar suas conclusões no Registro local do Windows e (opcionalmente) em um arquivo XML, para coleta e análise posteriores. O aplicativo do console também também pode ajudar na implementação das minimizações. Consulte *Usando a Ferramenta de detecção e minimização* INTEL-SA-00075 na página 2 para obter mais informações.

Se você for um administrador de rede que já usa o Software de instalação e configuração Intel® (Intel® SCS): a suíte Intel® SCS contém uma ferramenta de console alternativa, o utilitário Intel® SCS System Discovery. Sugerimos o uso dessa ferramenta se você já conhece as ferramentas do Intel® SCS ou gostaria de obter dados detalhados sobre a Intel® AMT. Consulte *Usando o utilitário Intel® SCS System Discovery*na página 111.

Minimização

As etapas de minimização descritas neste documento têm como objetivo impedir a ativação não autorizada e o uso de SKUs de gerenciabilidade da Intel, Intel® Active Management Technology (Intel® AMT), Intel® Standard Manageability (ISM) e Tecnologia Intel® para pequenas empresas (SBT), que não aplicaram a atualização do firmware para lidar com a vulnerabilidade.

Profissionais de TI podem usar as instruções a seguir como base para scripts ou tarefas em consoles de gerenciamento para distribuições em grande escala das etapas de minimização. A seguir, as etapas de procedimentos para implementar a minimização:

1. Cancelar o provisionamento de SKUs de gerenciabilidade Intel para reduzir tentativas de obtenção de privilégios do sistema por parte de invasores de rede sem privilégios
2. Desativar ou remover o Serviço de gerenciabilidade local (LMS) para reduzir tentativas de obtenção de privilégios do sistema por parte de invasores de rede sem privilégios
3. Opcionalmente, configurar restrições na configuração de gerenciabilidade local

A Intel recomenda enfaticamente que a primeira etapa em todos os caminhos de minimização seja remover a SKU de gerenciabilidade Intel, para lidar com a vulnerabilidade do escalonamento de privilégios de rede. Para os sistemas provisionados, o desprovisionamento deve ocorrer antes de desativar ou remover o LMS. De acordo com a disponibilidade do firmware da SKU de gerenciabilidade Intel atualizado, a Intel considera altamente recomendável a redução do escalonamento de privilégios locais, removendo ou desativando o LMS. Opcionalmente, como uma segunda camada de defesa contra a reinstalação ou reativação imprevistas do LMS, algumas opções de configuração da gerenciabilidade executadas através do SO podem ser desativadas no próprio sistema operacional (SO); contudo, essas restrições adicionais de configuração da gerenciabilidade local têm limitações quanto à respectiva permissão de reversão.

Nota: *a AMT 6.0.x não é compatível com o Modelo de controle de provisionamento/cliente baseado em Host e, consequentemente, não pode ser removida através da interface do sistema operacional local, via Ferramenta de detecção e minimização INTEL-SA-00075.* Nas plataformas usando o Firmware de gerenciabilidade 6.0.*x.x* ou 6.1.*x.x*, será necessário remover totalmente o provisionamento, usando o ACUConfig /full da Suíte Intel SCS ou os sistemas MEBx.

Para obter assistência na implementação das etapas de minimização contidas neste documento, entre em contato com Suporte ao cliente Intel; na seção Tecnologias, selecione Intel® Active Management Technology (Intel® AMT).

Usando a Ferramenta de detecção e minimização INTEL-SA-00075

O que é a Ferramenta de detecção e minimização INTEL-SA-00075?

A Ferramenta de detecção e minimização INTEL-SA-00075 pode ser utilizada por usuários locais ou por um administrador de TI para saber se um sistema está vulnerável à exploração do documentada no Intel Security Advisory (Alerta de segurança da Intel) INTEL-SA-00075. É possível utilizar a versão do console da ferramenta para executar as etapas de minimização.

A Ferramenta de detecção e minimização está disponível em duas versões.

- A primeira é uma ferramenta interativa de GUI que, ao ser executada, detecta os detalhes de hardware e software do dispositivo e fornece uma indicação da avaliação de riscos. Esta versão é recomendada para se obter a avaliação local do sistema.
- A segunda versão é um executável que pode fazer a avaliação de riscos e executar as etapas de minimização recomendadas. Como opção, é possível salvar as informações da descoberta no Registro do Windows* e/ou em um arquivo XML. Esta versão é mais conveniente para os administradores de TI que desejam fazer operações em massa de descoberta e minimização contínuas em várias máquinas.

Como obter a Ferramenta de detecção e minimização INTEL-SA-00075

Pacote de download da Ferramenta de detecção e minimização INTEL-SA-00075 está disponível em: https://www.intel.com/content/www/br/pt/support/technologies/000024133.html.

Requisitos do sistema

- Microsoft Windows* 7, 8, 8.1 ou 10
- Acesso administrativo ao sistema operacional local

Instalando a ferramenta

Instalação interativa

Execute a INTEL-SA-00075 Detection and Mitigation Tool.msi e siga as instruções da tela.

Instalação silenciosa

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

Esta ação instalará a Ferramenta de detecção e minimização INTEL-SA-00075 no diretório padrão,
`C:\Program Files (x86)\Intel\Intel-SA-00075 Detection and Mitigation Tool\`

Desinstalando a ferramenta

Desinstalação interativa

Execute a INTEL-SA-00075 Detection and Mitigation Tool.msi e siga as instruções da tela.

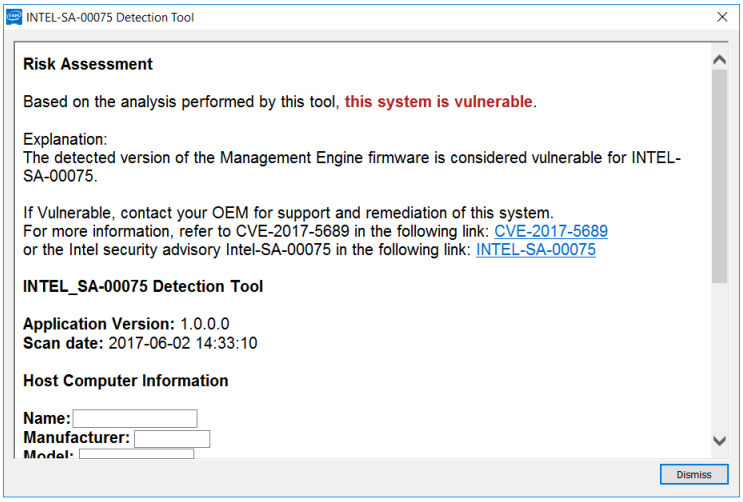
Desinstalação silenciosa

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

Execute a ferramenta da GUI

A INTEL-SA-00075-GUI.exe foi projetada para execução em um sistema individual. Quando executada, a ferramenta apresenta as informações de descoberta na tela.

Figura 1. Exemplo de saída da INTEL-SA-00075-GUI na tela



Execute a ferramenta do console

Execute `INTEL-SA-00075-console.exe` em um prompt de comando com privilégios administrativos.

Uso:

```
Intel-SA-00075-console.exe [[comando] | [opção...]]
```

Apenas um comando pode ser executado de cada vez. Se nenhum comando for emitido, será executado o recurso descoberta de comandos.

Tabela 1. Opções de linha de comando do console da INTEL-SA-00075

Comando de linha de comando	Funcionalidade
-Discover	Emite os resultados para o console e gravar os dados no registro.
-Unprovision [password], -u [password]	Remove todas as configurações da Intel AMT e desativa os recursos da Intel AMT; uma senha do usuário administrador para o dispositivo da Intel AMT pode ser usada e provavelmente obrigatória. Nota: chamar esse comando sem uma senha só funcionará com as versões do firmware afetadas pela INTEL-SA-00075 (6.1.*x*. *x*–11.6.*x*.*x* com um número de compilação inferior a 3000). Se estiver usando o firmware versões 6.1.x.*x*–11.6.*x*.*x* com um número de compilação acima de 3000, o desprovisionamento funcionará somente se uma senha for informada.
-DisableClientControlMode, -DisableCCM	Desativa permanentemente a opção do modo de Controle de cliente no dispositivo da Intel AMT. Após a execução deste comando, o dispositivo não poderá ser colocado no modo de Controle de cliente. NOTA: não existe um comando da CLI para reverter esta ação. AVISO: nem todas as plataformas podem reativar o CCM após desativado.
-DisableLMS	Desabilita o serviço LMS.

Opção de linha de comando	Funcionalidade
-n, - noregistry	Impede a gravação dos resultados no registro
-c, - noconsole	Impede a exibição dos resultados no console
-d, -delay <seconds>	Atraso em segundos antes de iniciar a execução. Se nenhum valor for especificado, a ferramenta não terá atraso.
-f, - writefile	Especifica a gravação dos resultados em um arquivo. O nome do arquivo usa o seguinte formato: <nomedocomputador>.xml
-p < filepath >, -filepath < filepath >	Caminho para armazenar o arquivo de saída. Se não for especificado, o arquivo será gravado no diretório a partir do qual a ferramenta é executada.
-h, -help, -?	Exibe essas opções de linha de comando e suas funções

-Discover

O comando discover envia as informações da descoberta para o console. Por padrão, ele também grava os dados da descoberta no registro. Se nenhum comando for emitido para a ferramenta do console, o comando discover será executado.

-Unprovision

Remove todas as configurações da Intel AMT e desativa os recursos da Intel AMT; uma senha opcional do usuário administrador para o dispositivo da Intel AMT pode ser usada.

Quando configurada, a Intel® AMT e ISM automaticamente escutam (detectam) o tráfego de gerenciamento através da rede do seu computador. Os sistemas vulneráveis ao conhecido problema de escalonamento de privilégios devem ser removidos por meio do comando unprovision para impedir o acesso não autorizado aos recursos de gerenciabilidade.

Chamar esse comando sem uma senha só funcionará com as versões de firmware afetadas pela INTEL-SA-00075 (6.1. *x.x*–11.6.*x.x* com um número de compilação inferior a 3000). Se estiver usando o firmware versões 6.1.x.*x*–11.6.*x.x* com um número de compilação acima de 3000, o desprovisionamento funcionará somente se uma senha for informada.

-DisableClientControlMode

A restrição de configuração -DisableClientControlMode é uma etapa opcional para os clientes que exigem uma camada secundária para proteger contra a reversão da minimização por um invasor sem privilégios, que obtém privilégios do administrador do sistema operacional. A reversão dessas opções é difícil, podem não ser aceita pelo fabricante do computador e talvez exija acesso físico ao sistema. Se você optar por fazer essa restrição de configuração adicional, execute-a antes de desativar o serviço LMS.

Procedimento para reativar o CCM

Se aceito pelo fabricante, você poderá redefinir a as SKUs de gerenciabilidade no BIOS, o que reativaria o CCM. Consulte o fabricante para saber se essa capacidade é compatível e para obter as etapas a seguir.

Nota: o fabricante pode fornecer as ferramentas que permitem configurar as configurações do BIOS através do sistema operacional. Se disponíveis, essas ferramentas podem permitir a redefinição das SKUs de gerenciabilidade da Intel no BIOS, sem precisar tocar fisicamente no computador. Consulte o fabricante para saber se eles fornecem uma ferramenta com essa funcionalidade.

-DisableLMS

O comando DisableLMS desativa o serviço LMS como uma etapa da minimização.

O que é LMS?

O Local Management Service (LMS) do aplicativo Intel® Management and Security é um serviço que permite que os aplicativos locais em execução nos dispositivos compatíveis com a Intel® AMT, Intel® SBA ou Intel® Standard Manageability utilizem a funcionalidade SOAP e WS-Management comuns. Ela escuta (detecta) as portas do Mecanismo de gerenciamento Intel® (16992, 16993, 16994, 16995, 623 e 664) e direciona o tráfego para o firmware através do driver da Interface do mecanismo de gerenciamento Intel®.

Outras considerações

Qualquer pessoa com privilégios de administrativos do sistema operacional poderá reinstalar o LMS, se ele for removido, ou reativar o serviço, se ele estiver desativado. Assim, é importante ter cuidado para evitar uma reinstalação ou reativação acidentais do LMS, enquanto existir vulnerabilidade no sistema. Por exemplo, o LMS pode ser reinstalado se você executar o instalador de software de gerenciamento da Intel, em algum momento posterior.

Figura 2. Exemplo de saída do Console da INTEL-SA-00075

```
Ferramenta Descoberta da INTEL-SA-00075
Versão do aplicativo: <versão do aplicativo>
Data da verificação: <data e hora>

*** Informações sobre o Computador Host ***
Nome do computador: <nome do computador>
Fabricante: <fabricante do computador>
Modelo: <modelo do computador>
Processador: <modelo do processador>
Versão do Windows: <versão do Windows*>

*** Informações sobre o Mecanismo de Gerenciamento ***
Versão: <versão do firmware do Mecanismo de gerenciamento Intel>
SKU: <recurso de gerenciabilidade, se estiver presente>
Estado: <estado de provisionamento do ME>
Driver instalado: <Verdadeiro/Falso>
Modo de controle: <Nenhum/ACM/CCM>
```

```
CCM está desativado: <Verdadeiro/Falso/Desconhecido >
EHBC ativado <Verdadeiro/Falso>
Estado do LMS: <Em execução/Parado/Ausente>
Tipo de inicialização do LMS: <Inicialização/Sistema/Auto/Manual/Desativado/Ausente>
Estado do MicroLMS: <Em execução/Parado/Ausente>
Tipo de inicialização do MicroLMS:
<Inicialização/Sistema/Auto/Manual/Desativado/Ausente>
É SPS: <Verdadeiro/Falso>


*** Avaliação de riscos ***
Com base na análise executada por esta ferramenta,
<este sistema está vulnerável /
este sistema não está vulnerável /
este sistema não está vulnerável; SKU não - Intel /
este sistema não está vulnerável; a versão do FW do ME não está afetada /
este sistema não está vulnerável; a SKU do ME não está afetado /
este sistema não está vulnerável; o SMBIOS indica que este é uma AKU do consumidor /
este sistema não está vulnerável; o sistema está executando o FW do SPS (Firmware de
Serviços de plataforma de servidor) /
o firmware deste sistema foi atualizado e o sistema está em estado desprovisionado /
o firmware deste sistema foi atualizado e o sistema está em estado de
provisionamento /
Consulte o OEM /
o risco deste sistema é desconhecido>

Se vulnerável, entre em contato com o seu OEM para obter suporte e correção deste
sistema.

*** Para obter mais informações ***
Consulte CVE-2017-5689 em:
     https://nvd.nist.gov/vuln/detail/CVE-2017-5689

ou o Alerta de segurança da Intel, Intel-SA-00075, em:
     https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-
00075&languageid=en-fr
```

A lógica usada para determinar uma avaliação de riscos está descrita em Tabela 2.

Tabela 2. Significado da avaliação de riscos na saída

Mensagem	Significado
Vulnerável	A versão detectada do firmware do mecanismo de gerenciamento é considerada vulnerável para INTEL-SA-00075.
Não vulnerável	O sistema atende aos critérios de "Invulnerabilidade" descritos em *Como identificar os sistemas impactados por meio da* Ferramenta de descoberta da INTEL-SA-00075 na página 8.
O firmware deste sistema foi atualizado e o sistema está em estado desprovisionado	O firmware detectado neste sistema tem a correção para INTEL-SA-00075. Certifique-se de que as ferramentas INTEL-SA-00075 tenham sido utilizadas para executar um desprovisionamento completo do sistema, antes de refazer o provisionamento. Esta ação removerá todos os parâmetros de configuração não autorizados.
O firmware deste sistema foi atualizado e o sistema está em estado de provisionamento	O firmware detectado neste sistema tem a correção para INTEL-SA-00075. Se o sistema foi provisionado antes da atualização do firmware, um desprovisionamento completo e novo provisionamento do sistema removerão quaisquer parâmetros de configuração não autorizados.

Mensagem	Significado
Consulte o OEM	As informações detectadas no SMBIOS do OEM mostram uma SKU de gerenciabilidade, mas a ferramenta não recebeu uma resposta ao solicitar dados detalhados do seu computador. Isso pode ter sido causado pela ausência de um driver da Interface do mecanismo de gerenciamento. Consulte o OEM para saber se o modelo do computador está afetado.
Desconhecido	A ferramenta não recebeu uma resposta válida ao solicitar os dados de inventário de hardware do seu computador. Entre em contato com o fabricante do sistema para obter ajuda na determinação da vulnerabilidade deste sistema. Esta mensagem pode ser recebida em uma plataforma de servidor sem um Driver PMX instalado. Este driver pode não estar disponível em todas as versões do sistema operacional Windows. Se o driver não estiver presente, a solução recomendada é executar o aplicativo spsInfo ou spsManuf fornecido com a versão do Firmware de SPS. Os dois aplicativos instalarão o Driver PMX.

Resultados

Nota: a quantidade de dados retornada pelo comando Discover da INTEL-SA-00075 dependerá se a pilha de drivers de gerenciabilidade da Intel está carregada no sistema. Se o driver da Interface do mecanismo de gerenciamento Intel® e do Serviço de gerenciamento local (LMS) do aplicativo de segurança estiverem presentes, haverá um conjunto mais detalhado de dados disponível. Alguns campos podem não ser aceitos pelo fabricante.

Local do registro

Os valores da tabela de resultados podem ser encontrados na seguinte chave do registro:

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

XML

Se você optar por gravar os resultados em um arquivo XML, esse arquivo será armazenado no diretório a partir do qual o INTEL-SA-00075-console.exe for executado ou do caminho especificado nas opções de linha de comando. Estão incluídas informações, como o inventário de hardware, sistema operacional, a presença do LMS. Se a AMT estiver presente, estará incluída a lista de hashes de certificados padrão e personalizado encontrados. Essa lista pode ser usada para comparar os hashes esperados com o que está armazenado na AMT.

Códigos de retorno de console

Tabela 3. Códigos de retorno do console da INTEL-SA-00075

Número	Significado
0	NOTVULNERABLE (If Discover command was run) | STATUS_OK
2	MACHINE_STATE_UNCONFIGURED
30	CLIENT_CONFIG_NOT_SUPPORTED

Número	Significado
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

Tabela 4. Valores de saída do console da INTEL-SA-00075

Valor	Localização	Descrição
Application Version (Versão do aplicativo)		A versão da ferramenta de verificação utilizada
Scan Date (Data da verificação)		Data e hora da verificação
Computer Name (Nome do computador)		Nome do computador verificado
Computer Manufacturer (Fabricante do computador)	Inventário de hardware	Fabricante do computador
Computer Model (Modelo de computador)		Modelo do computador
Processor (Processador)		Modelo do processador do computador
ME Version (Versão do ME)	Informação sobre o firmware do ME	Um valor de sequência com o número completo da versão do firmware do ME, no seguinte formato: Major.Minor.Hotfix.Build
ME SKU (SKU do ME)		Se estiver presente, a capacidade de gerenciamento do sistema
ME Provisioning State (Estado de provisionamento do ME)		Estado da configuração do ME Nada detectado Não provisionado Provisionando no processo Provisionado
ME Driver Installed (Driver do ME instalado)		Valor Falso/Verdadeiro, se o driver de MEI estiver presente no computador
EHBC Enabled (EHBC ativado)		Valor Falso/Verdadeiro, se o sistema tiver capacidade para o método de provisionamento da Configuração Baseada em Host Embarcado
LMS state (Estado do LMS)		Informação se o serviço LMS está em execução, não executando ou ausente
LMS startup type (Tipo de inicialização do LMS)		Informação se o tipo de inicialização do LMS é Ausente, inicialização, Sistema, Auto, Manual ou Desativado
MicroLMS state (Estado do MicroLMS)		Informação se o Serviço MicroLMS está em execução, não executando ou ausente
MicroLMS startup type (Tipo de inicialização do MicroLMS)		Informação se o tipo de inicialização do MicroLMS é Ausente, Inicialização, Sistema, Auto, Manual ou Desativado
Control Mode (Modo de controle)		O modo de configuração do ME Nenhum, ACM ou CCM
Is CCM Disabled (CCM está desabilitado)		Status Verdadeiro/Falso/Desconhecido para o modo de Controle do cliente desativado
Is SPS (É SPS)		A plataforma é um sistema de Serviços de plataforma de servidor (SPS) não vulnerável?
*** Avaliação de riscos ***	Avaliação de riscos	Consulte *Tabela 2. Significado da avaliação de riscos na saída*

Como identificar os sistemas impactados por meio da Ferramenta de descoberta da INTEL-SA-00075

Sistemas afetados são definidos como tendo uma versão do firmware do Mecanismo de gerenciamento Intel® afetado e contendo um dos três conjuntos de recursos de gerenciabilidade, conforme definido em Tabela 5.

Nota: as plataformas de Serviços de plataforma de servidor (SPS) não são vulneráveis à INTEL-SA-00075. As plataformas SPS têm o firmware em execução no Mecanismo de gerenciamento (ME) (parte do PCH) em plataformas de servidor. Esse firmware é diferente do firmware de gerenciabilidade Intel (também executando no ME) em plataformas de PC/Workstation.

Tabela 5. Critérios para determinar se um sistema está vulnerável a INTEL-SA-00075, por meio da ferramenta de descoberta da INTEL-SA-00075

Nome do valor	Vulnerável	Não vulnerável
`SKU do ME`	Gerenciabilidade completa da Intel® AMT Intel® Standard Manageability Vantagem Intel® para pequenas empresas	Valores de SKUs do ME ausentes na lista de vulneráveis à esquerda - ou - Valores de SKUs do ME à esquerda com uma versão de firmware que não é vulnerável
`Versão do ME`	ME versões 6.x.x.x – 11.7.x.x com um valor de compilação inferior a 3000 Exemplo: 9.5.0.22.**1760**	Versões do ME: • 6.x.x.x – 11.7.x.x com um valor de compilação superior ou igual a 3000 o Exemplo: 11.6.0.2.**3264** • 2.x.x.x. — 5.x.x.x • 11.7.x.x ou acima

Nota: Tecnologia Intel® para pequenas empresas é a SKU de gerenciabilidade para a Vantagem Intel® para pequenas empresas.

Estendendo o inventário do Hardware do Microsoft* SCCM para incluir os resultados da ferramenta do console da INTEL-SA-00075

Ao optar por armazenar os resultados da ferramenta do console da Intel-SA-00075 no Registro do Windows, você poderá aproveitar a extensibilidade de inventário de hardware do Microsoft * SCCM para importar os resultados. Isso permitirá a criação de coleções no SCCM para computadores de destino, para correção ou atualizações de firmware. Para isso, faça o seguinte:

1. Adicione classes de inventário de hardware ao arquivo configuration.mof do SCCM.
2. Habilite essas novas classes de inventário de hardware na sua configuração de cliente.
3. Crie um pacote de software para implantar e executar a Ferramenta do console da INTEL-SA-00075 (`Intel-SA-00075-console.exe`).
4. Crie uma sequência de tarefas para executar o pacote de software.

Modificação do arquivo MOF

Nota: se existir um servidor central em seu ambiente, altere o arquivo MOF nesse servidor. Caso contrário, faça essas alterações em cada um dos servidores primários.

1. Localize o arquivo configuration.mof. Ele é normalmente encontrado em \Program Files\Microsoft Configuration Manager\inboxex\clifiles.src\hinv\
2. Faça uma cópia de backup.
3. Edite o arquivo configuration.mof, rolando para baixo até o final do arquivo, posicione o cursor acima desta linha:

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

4. Cole o conteúdo das alterações efetuadas no arquivo MOF da página 13 e 14 neste documento, acima da linha da etapa 3.
5. Salve e feche o arquivo.
6. Abra um prompt de comando em execução como administrador no diretório contendo o configuration.mof.
7. Execute o mofcomp sem opções de direcionando o arquivo modificado configuration.mof.

Mudanças do inventário do hardware

Nota: após efetuadas, essas alterações precisarão de algum tempo para se propagar para seus clientes, antes de esses novos itens aparecerem no inventário de hardware. O tempo necessário dependerá da configuração do ambiente.

1. Crie um novo arquivo denominado INTEL-SA-00075.mof.
2. Cole o conteúdo de Importação do Inventário de Hardware da INTEL-SA-00075 na página 165 no arquivo recém-criado e salve.
3. Abra o Console do Configuration Manager.
4. Administração > Configurações do Cliente > Configurações do Cliente Padrão.
5. Clique com o botão direito em Configurações do Cliente Padrão > Propriedades.
6. Selecione Inventário de Hardware > Definir Classes.
7. Clique em Importar.
8. Navegue até o arquivo INTEL-SA-00075.mof > Abrir.
9. Verifique se a opção "Importar classes de inventário de hardware e configurações de classe de inventário de hardware" está marcada.
10. Clique em Importar.
11. OK > OK.
12. O SCCM registra as alterações efetuadas no inventário de Hardware no arquivo dataldr.log.

Criar pacote do SCCM

1. Crie o arquivo de lote da página 15 e coloque-o em uma pasta com o arquivo da ferramenta do console da INTEL-SA-00075.
2. Abra o Console do Configuration Manager.
3. Biblioteca de Software > Pacotes.
4. Clique com botão direito em Pacotes > Criar Pacote.
5. Nome: Intel-SA-00075.
6. Marque a opção: Este pacote contém arquivos de origem.
7. Procure a pasta do pacote criada na etapa 1.
8. Avançar.
9. Marque a opção: Não criar um programa.
10. Avançar > Avançar > Fechar.

11. Distribua o pacote para os pontos de distribuição adequados.

Criar sequência de tarefas do SCCM

1. Abra o Console do Configuration Manager.
2. Biblioteca de Software > Sistemas Operacionais.
3. Clique com botão direito em Sequências de Tarefas > Criar Sequência de Tarefas.
4. Marque a opção Criar uma nova sequência de tarefa personalizada.
5. Avançar.
6. Digite um nome da Intel-SA-00075.
7. Avançar > Avançar > Fechar.
8. Clique com botão direito na sequência de tarefas da Intel-SA-00075 e clique em Editar.
9. Adicionar > Geral > Executar Linha de Comando.
10. Digite Intel-SA-00075.bat no campo Linha de comando.
11. Marque a caixa Pacote e selecione Procurar.
12. Selecione o pacote Intel-SA-00075 criado anteriormente > OK.
13. Clique em OK.

Usando o utilitário Intel® SCS System Discovery

O que é o utilitário Intel® SCS System Discovery?

O utilitário Intel® SCS System Discovery é um componente da suíte Software de instalação e configuração Intel® (Intel® SCS), que fornecerá detalhes específicos do hardware e software existentes em um sistema, compatíveis com a Intel® Active Management Technology (Intel® AMT), Intel® Standard Manageability (ISM) ou Tecnologia Intel® para pequenas empresas. Quando executado, ele pode salvar os resultados no Registro do Microsoft Windows e/ou em um arquivo XML. Estas informações podem ser usadas para encontrar os sistemas para os quais direcionar as atualizações de firmware ou implementar minimizações.

Como obter o utilitário Intel® SCS System Discovery

O pacote de download do utilitário Intel® SCS System Discovery está disponível em https://downloadcenter.intel.com/download/26691/Intel-SCS-System-Discovery-Utility.

Determinando a versão do firmware de gerenciabilidade, usando o utilitário Intel® SCS System Discovery

A saída do utilitário Intel® SCS System Discovery pode ser usada para saber a versão do firmware do sistema e se o sistema é uma SKU de gerenciabilidade. Estas informações são fornecidas na seção da saída do `ManageabilityInfo`. Para obter instruções sobre como executar a ferramenta, leia a seção de *Executar o utilitário Intel® SCS System Discovery*, na página 12.

O valor de `FWVersion` contém a versão do firmware atualmente existente no dispositivo. O valor de `AMTSSKU` contém a SKU de gerenciabilidade compatível, se presente. Revise os valores de `FWVersion` e `AMTSKU` para conhecer a vulnerabilidade do seu sistema, conforme descrita em Tabela 6.

Tabela 6. Critérios para saber se um sistema está vulnerável a INTEL-SA-00075, por meio do utilitário Intel® SCS System Discovery

Nome do valor	Vulnerável	Não vulnerável
AMTSKU	Gerenciabilidade da Intel(R) AMT completa Intel(R) Standard Manageability Vantagem Intel(R) para pequenas empresas Exemplo de saída: <ManageabilityInfo> <AMTSKU>**Intel(R) Full AMT Manageability**</AMTSKU> <AMTversion>**11.0.0**</AMTversion> <FWVersion>**11.0.0.1202**</FWVersion>	Valor de AMTSKU não está presente na saída - ou - Valores de AMTSKU à esquerda, com uma versão de firmware que não está vulnerável Exemplo de saída: <ManageabilityInfo> <FWVersion>**9.0.13.1402**</FWVersion>
FWVersion	Versões do firmware da SKU de gerenciabilidade da Intel® 6.x.x.x – 11.7.x.x com um valor de compilação inferior a 3000 Exemplo: 9.5.0.22.**1760**	Versões do firmware da SKU de gerenciabilidade da Intel®: • 6.x.x.x – 11.7.x.x com um valor de compilação superior ou igual a 3000 o Exemplo: 11.6.0.2.**3264** • 2.x.x.x. — 5.x.x.x • 11.7.x.x ou acima

Nota: Tecnologia Intel® para pequenas empresas é a SKU de gerenciabilidade para a Vantagem Intel® para pequenas empresas.

Execução do utilitário Intel® SCS System Discovery

Salvar os dados apenas no registro

Execute o seguinte comando em um prompt de comando com direitos administrativos, para executar o utilitário Intel® System SCS Discovery e gravar dados no registro:

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

Salvar os dados apenas em um arquivo XML

Use o seguinte comando para executar o utilitário Intel® SCS System Discovery e salvar os dados em um arquivo XML:

```
SCSDiscovery.exe SystemDiscovery <filename and path> /noregistry
```

O caminho e nome do arquivo podem ser uma localização local no sistema ou um compartilhamento de rede. Se você optar por usar um compartilhamento de rede, verifique se a conta executando o utilitário Intel® SCS System Discovery tem permissões de gravação nesse compartilhamento de rede. Se você não especificar um nome de arquivo e um caminho, o FQDN do sistema será usado para o nome do arquivo XML e o arquivo será armazenado no diretório que contém o utilitário Intel® SCS System Discovery.

Salvar os dados no registro e em um arquivo XML

Use o seguinte comando para executar o utilitário Intel® SCS System Discovery para salvar os dados no registro e em um arquivo XML

```
SCSDiscovery.exe SystemDiscovery <nome do arquivo e caminho>
```

Como no exemplo anterior, se você não especificar um nome de arquivo e um caminho, o FQDN do sistema será usado para o nome do arquivo XML e o arquivo será armazenado no diretório que contém o utilitário Intel(R) SCS System Discovery.

Resultados do utilitário Intel(R) SCS System Discovery

A quantidade de dados retornada pelo utilitário Intel® SCS System Discovery dependerá se a pilha de drivers de gerenciabilidade da Intel está carregada no sistema. Se o driver da Interface do mecanismo de gerenciamento Intel® e do Serviço de gerenciamento local (LMS) do aplicativo de segurança estiverem presentes, haverá um conjunto mais detalhado de dados disponível. Os resultados descritos abaixo se concentrarão em apenas alguns campos de dados principais, relevantes para o problema de escalonamento de privilégios conhecidos. Para obter detalhes adicionais sobre os outros campos de dados, consulte a documentação do utilitário Intel® SCS System Discovery. Alguns campos podem não ser aceitos pelo fabricante.

Resultados do registro

Os resultados gravados no registro podem ser encontrados na seguinte localização:
`HKLM\Software\Intel\Setup e Configuration Software\SystemDiscovery`

Principais valores:

Nome do valor	Subchave do Registro	Descrição do valor
FWVersion	ManageabilityInfo	Versão do firmware do Mecanismo de gerenciamento Intel®
AMTSKU	ManageabilityInfo	Recurso de gerenciabilidade aceito, se existir

Resultados do arquivo XML

A versão do firmware do Mecanismo de gerenciamento Intel® é encontrada no seguinte caminho, no XML:

```
<SystemDiscovery>
       <ManageabilityInfo>
              <FWVersion> Número da Versão </FWVersion>
```

Recurso de gerenciabilidade com suporte no sistema, se houver, encontra-se no seguinte caminho, no XML:

```
<SystemDiscovery>
       <ManageabilityInfo>
              <AMTSKU> Nome do Recurso de Gerenciabilidade </AMTSKU>
```

Importação de dados de descoberta de sistema para o inventário de hardware do SCCM

O processo de coleta de dados de descoberta do sistema pode ser automatizado com o dispositivo de expansão Intel® SCS para o Microsoft* System Center Configuration Manager (SCCM). Quando instalado, esse complemento estenderá automaticamente o inventário de hardware do SCCM para incluir dados de descoberta de sistema, além de criar sequências de tarefas que podem ser usadas para executar a descoberta do sistema em relação a coleções de sistemas. As informações coletadas por meio desse processo, em seguida, podem ser usadas para criar coleções do SCCM para enviar atualizações de firmware ou minimizações para os sistemas afetados.

O pacote de download do dispositivo de expansão Intel® SCS para o Microsoft SCCM está disponível em https://downloadcenter.intel.com/download/26506/Intel-SCS-Add-on-for-Microsoft-System-Center-Configuration-Manager.

Alterações no arquivo 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 ====
```

Importação do Inventário de Hardware da 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;
};
```

Arquivo INTEL-SA-00075.bat lote

```
@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%
```

Exemplos de consulta de coleta

Computadores aprovisionados

```
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 em execução