Guide de l'outil de détection et d'atténuation des risques INTEL-SA-00075

Technologie d'administration active Intel®, Intel® Standard Manageability (ISM) et technologie Intel® Small Business Technology (SBT)

Instructions de détection et d'atténuation des risques INTEL-SA-00075

Révision 1.1 – 20 juillet 2017

Introduction

Ce document vous guidera au long de plusieurs processus permettant de détecter et neutraliser la vulnérabilité de sécurité décrite dans INTEL-SA-00075. Lire l'avis de sécurité public à https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr pour plus d'informations.

Si vous êtes utilisateur d'un PC unique et souhaitez déterminer son état : nous fournissons l'application de détection INTEL-SA-00075 dotée d'une GUI (Intel-SA-00075-gui.exe) pour l'analyse locale d'un système unique ou autonome.

Si vous souhaitez déterminer l'état et/ou appliquer des mesures d'atténuation des risques sur plusieurs machines : nous avons fourni la console de l'outil de détection et d'atténuation des risques INTEL-SA-00075 (Intel-SA-00075-console.exe). Cet outil peut effectuer une analyse et écrire ses conclusions dans le registre de Windows local et (facultatif) dans un fichier XML, pour collecte et analyse ultérieures. L'application de la console peut également aider à implémenter des mesures d'atténuation des risques. Voir *Utilisation de l'outil de détection et d'atténuation* des risques INTEL-SA-00075, page 2, pour plus d'informations.

Si vous êtes un administrateur réseau qui utilise déjà le logiciel pour installer et configurer Intel® SCS : la suite Intel® SCS contient un autre outil de console, l'utilitaire Intel® SCS System Discovery. Nous recommandons d'utiliser cet outil si vous vous êtes déjà familiarisé avec les outils Intel® SCS ou si vous souhaitez obtenir des données détaillées sur la technologie d'administration active Intel®. Voir *Utilisation de l'utilitaire de découverte de système* Intel® SCS, page 121.

Atténuation des risques

Les étapes d'atténuation des risques décrites dans ce document sont destinées à empêcher l'activation et l'utilisation non autorisées des produits d'administration Intel, de la technologie d'administration active Intel®, d'Intel® Standard Manageability (ISM) et de la technologie Intel® Small Business Technology (SBT), sur lesquels la mise à jour du microprogramme résolvant la vulnérabilité n'a pas été installée.

Les professionnels de services informatiques peuvent utiliser ces instructions comme base de scripts ou de tâches pour consoles d'administration pour le déploiement à grande échelle des étapes d'atténuation des risques. Les étapes de la procédure de mise en œuvre de l'atténuation des risques sont les suivantes :

1. Annulation de la mise en service de clients d'administration Intel pour empêcher les intrus attaquant le réseau d'obtenir des privilèges système
2. Désactiver ou supprimer le service d'administration local (LMS) afin d'empêcher les intrus attaquant le réseau d'obtenir des privilèges système
3. Configuration des restrictions de configuration d'outils d'administration (facultatif)

Intel recommande vivement comme première étape des mesures d'atténuation des risques d'annuler la mise en service des produits d'administration Intel pour résoudre le problème d'escalade de privilèges réseau. Pour les systèmes déployés, l'annulation de la mise en service doit être effectuée avant la désactivation ou la suppression du LMS. En attendant la disponibilité de la mise à jour du microprogramme d'administration Intel, Intel recommande fortement de prendre des mesures d'atténuation des risques d'escalade des privilèges locaux en supprimant ou en désactivant le LMS. Le cas échéant, comme seconde couche de protection contre la réinstallation ou la réactivation accidentelles du LMS, certaines options de configuration de l'administration effectuées par le biais du système d'exploitation peuvent être désactivées dans le système d'exploitation (SE). Toutefois, ces restrictions de configuration des outils d'administration possèdent des contraintes concernant les possibilités d'inversion.

Remarque : la technologie d'administration active 6.0.*x* ne prend pas en charge le modèle de contrôle d'approvisionnement/contrôle client et, par conséquent, son service ne peut pas être annulé dans l'interface du système d'exploitation local à l'aide de l'outil de détection et d'atténuation des risques INTEL-SA-00075. Pour les plates-formes utilisant le microprogramme d'administration 6.0.*x.x* ou 6.1.*x.x*, il sera nécessaire d'annuler totalement la mise en service à l'aide de la fonctionnalité ACUConfig /full de la suite Intel® SCS ou de l'extension MEBx du système.

Pour obtenir de l'assistance sur l'implémentation de la procédure d'atténuation des risques fournie dans ce document, veuillez contacter l'assistance à la clientèle Intel ; dans la section Technologies, sélectionnez Technologie d'administration active Intel® (Intel® AMT).

Utilisation de l'outil de détection et d'atténuation des risques INTEL-SA-00075

Qu'est-ce que l'outil de détection et d'atténuation des risques INTEL-SA-00075 ?

L'outil de détection et d'atténuation des risques INTEL-SA-00075 peut être utilisé par les utilisateurs locaux ou un administrateur informatique afin de déterminer si un système est vulnérable à la faille de sécurité documentée dans l'avis de sécurité public Intel Security Advisory INTEL-SA-00075. La version console de l'outil peut être utilisée pour effectuer les étapes d'atténuation des risques.

L'outil de détection et d'atténuation des risques est proposé en deux versions.

- La première est un outil interactif utilisant une interface graphique qui, lorsqu'il est exécuté, identifie les détails matériels et logiciels de l'ordinateur et fournit une évaluation des risques. Cette version est recommandée lorsque l'évaluation locale du système est nécessaire.
- La deuxième version est un fichier exécutable de console qui peut réaliser l'évaluation des risques et les étapes d'atténuation des risques recommandées. Elle peut éventuellement enregistrer les informations de détection dans le registre Windows* et/ou dans

un fichier XML. Cette version est plus pratique pour les administrateurs informatiques qui souhaitent effectuer des opérations de détection et d'atténuation des risques en bloc sur plusieurs ordinateurs.

Obtenir l'outil de détection et d'atténuation des risques INTEL-SA-00075

Le package de téléchargement de l'outil de détection et d'atténuation des risques INTEL-SA-00075 est disponible à : https://www.intel.fr/content/www/fr/fr/support/technologies/000024133.html.

Configuration requise

- Microsoft Windows* 7, 8, 8.1 ou 10
- Accès d'administrateur au système d'exploitation local

Installation de l'outil

Installation interactive

Exécutez INTEL-SA-00075 Detection and Mitigation Tool.msi et suivez les instructions à l'écran.

Installation en mode silencieux

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

Cela installe l'outil de détection et d'atténuation des risques INTEL-SA-00075 dans le répertoire par défaut, `C:\Program Files (x86)\Intel\Intel-SA-00075 Detection and Mitigation Tool\`

Désinstallation de l'outil

Désinstallation interactive

Exécutez INTEL-SA-00075 Detection and Mitigation Tool.msi et suivez les instructions à l'écran.

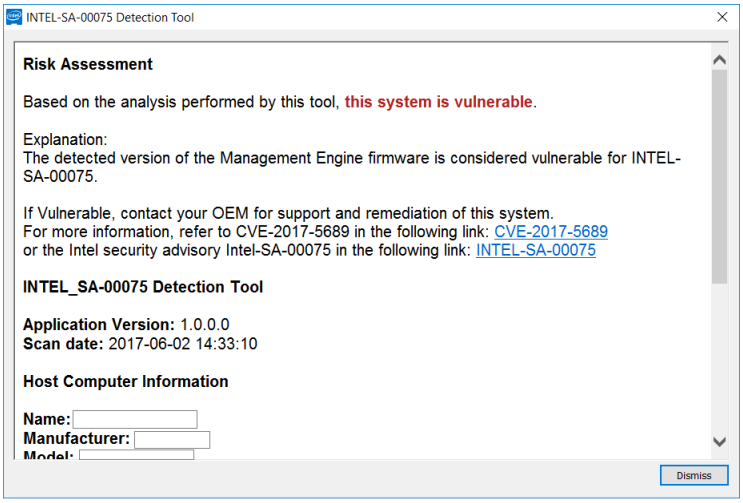
Désinstallation en mode silencieux

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

Exécution de l'outil à interface graphique

Le fichier INTEL-SA-00075-GUI.exe est conçu pour fonctionner sur un seul système. Lors de l'exécution, l'outil affiche les informations de détection à l'écran.

Figure 1. Exemple de sortie de la GUI INTEL-SA-00075 à l'écran



Exécution de l'outil de console

Exécutez `INTEL-SA-00075-console.exe` depuis une invite de commande en tant qu'administrateur.

Syntaxe :

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

Une seule commande peut être exécutée à la fois. Si aucune commande n'est fournie, la commande de détection est exécutée.

Tableau 1. Commutateurs de ligne de commande de la console INTEL-SA-00075

Commande de ligne de commande	Fonctionnalité
-Discover	Envoie les résultats de la sortie sur la console et écrit les données dans le registre.
-Unprovision [mot de passe], -u [password]	Supprime tous les paramètres de la technologie d'administration active Intel et désactive ses fonctions ; un mot de passe d'administrateur de l'ordinateur utilisant la technologie d'administration active Intel peut être utilisé et peut s'avérer nécessaire. REMARQUE : l'appel de cette commande sans mot de passe ne fonctionne qu'avec les versions de microprogramme affectées par INTEL-SA-00075 (6.1.*x.x*–11.6.*x.x* avec un numéro de build de moins de 3000). Si vous utilisez un microprogramme de version 6.1.x.*x*–11.6.*x.x* possédant un numéro de build supérieur à 3000, l'annulation de la mise en service fonctionne uniquement si un mot de passe est fourni.
-DisableClientControlMode, -DisableCCM	Désactive définitivement l'option du mode de contrôle client sur l'ordinateur utilisant la technologie d'administration active Intel. Après l'exécution de cette commande, l'ordinateur ne peut pas être mis en mode de contrôle client. REMARQUE : il n'existe pas de commande de ligne de commande pour annuler cette action. AVERTISSEMENT : toutes les plates-formes ne peuvent pas réactiver le mode de contrôle client une fois désactivé.
-DisableLMS	Désactive le service LMS.

Option de ligne de commande	Fonctionnalité
-n, -noregistry	Empêche d'écrire les résultats dans le registre
-c, -noconsole	Empêche d'afficher les résultats sur la console
-d, -delay <secondes>	Délai en secondes avant que l'exécution démarre. Si aucune valeur n'est spécifiée, l'outil n'utilisera aucun délai.
-f, -writefile	Spécifie d'écrire les résultats dans un fichier. Le nom de fichier utilise le format suivant : <nom de l'ordinateur>.xml
-p <filepath>, -filepath <filepath>	Le chemin d'accès pour stocker le fichier de sortie. Si aucun chemin d'accès n'est spécifié, le fichier sera écrit dans le répertoire à partir duquel l'outil est exécuté.
-h, -help, -?	Affiche ces commutateurs de ligne de commande et leurs fonctions

-Discover

La commande discover affiche les informations de détection sur la console. Par défaut, elle écrit également les données de détection dans le registre. Si aucune commande n'est fournie à l'outil de console, la commande discover est exécutée.

-Unprovision

Supprime tous les paramètres de la technologie d'administration active Intel et désactive ses fonctions ; un mot de passe facultatif d'administrateur de l'ordinateur utilisant la technologie d'administration active Intel peut être utilisé.

Lorsqu'elles sont configurées, la technologie d'administration active Intel et ISM écoutent automatiquement le trafic d'administration sur votre réseau d'ordinateurs. Les systèmes vulnérables au problème d'escalade des privilèges connu doivent être retirés du service à l'aide de la commande « unprovision » afin d'empêcher tout accès non autorisé aux fonctions d'administration.

L'appel de cette commande sans mot de passe ne fonctionne qu'avec les versions de microprogramme affectées par INTEL-SA-00075 (6.1.*x*.*x*–11.6.*x*.*x* avec un numéro de build de moins de 3000). Si vous utilisez un microprogramme de version 6.1.x.*x*–11.6.*x*.*x* possédant un numéro de build supérieur à 3000, l'annulation de la mise en service fonctionne uniquement si un mot de passe est fourni.

-DisableClientControlMode

La restriction de configuration -DisableClientControlMode est une étape facultative pour les clients qui exigent une couche secondaire pour se protéger contre l'inversion d'atténuation des risques par un attaquant non autorisé qui parvient à obtenir des droits d'administrateur sur le système d'exploitation. L'inversion de ces options est difficile, il est possible qu'elle ne soit pas prise en charge par le constructeur de l'ordinateur et peut nécessiter un accès physique au système. Si vous choisissez d'effectuer cette restriction de configuration supplémentaire, elle doit être effectuée avant la désactivation du service LMS.

Étapes pour réactiver le mode de contrôle client

Si cette opération est prise en charge par le constructeur de votre ordinateur, il est possible que vous puissiez rétablir les services d'administration Intel à partir du BIOS, ce qui réactiverait le mode de contrôle client. Consultez le constructeur pour savoir si cette fonctionnalité est prise en charge et obtenir les étapes à suivre.

Remarque : il est possible que le constructeur de votre ordinateur puisse fournir des outils qui vous permettent de configurer les paramètres du BIOS par le biais du système d'exploitation. Ces outils, s'ils sont disponibles, pourraient vous permettre de rétablir les services d'administration Intel à partir du BIOS sans avoir à toucher physiquement l'ordinateur. Consultez votre constructeur pour savoir s'il fournit un outil possédant cette fonctionnalité.

-DisableLMS

La commande DisableLMS désactive le service LMS dans le cadre de l'atténuation des risques.

Qu'est-ce que le service LMS ?

Le service d'administration local (LMS) de l'application d'administration et de sécurité Intel® est un service qui permet aux applications locales exécutées des ordinateurs pris en charge utilisant la technologie d'administration active Intel®, Intel® Small Business Advantage ou Intel® Standard Manageability d'utiliser les fonctionnalités SOAP et de WS-Management communes. Il écoute les ports Intel® ME (Manageability Engine) (16992, 16993, 16994, 16995, 623 et 664) et achemine le trafic vers le microprogramme à l'aide du pilote Intel® MEI.

Considérations supplémentaires

Toute personne disposant de privilèges d'administration sur le système d'exploitation sera en mesure de réinstaller le LMS s'il est supprimé, ou de réactiver le service s'il est désactivé. Par conséquent, il est important d'être prudent afin d'éviter une réinstallation ou une réactivation accidentelle du service LMS alors que le système est toujours vulnérable. Par exemple, le service LMS pourrait être réinstallé si vous exécutez à l'avenir le programme d'installation du logiciel d'administration Intel.

Figure 2. Exemple de sortie de console INTEL-SA-00075

```
Outil INTEL-SA-00075 Discovery
Version de l'application : <version de l'application>
Date d'analyse : <date et heure>

*** Informations sur l'ordinateur hôte ***
Nom de l'ordinateur : <nom de l'ordinateur>
Constructeur : <constructeur de l'ordinateur>
Modèle : <modèle de l'ordinateur>
Processeur : <modèle du processeur>
Version de Windows : <version de Windows*>

*** Informations sur le moteur de gestion ***
Version : <version sur le microprogramme du moteur de gestion Intel>
Référence : <fonctionnalité d'administration, le cas échéant>
État : <état de mise en service du moteur de gestion>
Pilote installé : <Vrai/Faux>
Mode de contrôle : <aucun/ACM/CCM>
CCM est désactivé : <Faux/Vrai/inconnu>
EHBC activé <Faux/Vrai>
État du LMS : <en cours d'exécution/arrêté/absent>
Type de démarrage LMS : <Démarrage/Système/Sutomatique/Manuel/Désactivé/Absent>
État MicroLMS : <en cours d'exécution/arrêté/Absent>
Type de démarrage MicroLMS : <Démarrage/Système/Sutomatique/Manuel/Désactivé/Absent>
Est SPS : <Faux/Vrai>


*** Évaluation des risques ***
En fonction de l'analyse effectuée par cet outil,
< ce système est vulnérable /
ce système n'est pas vulnérable /
ce système n'est pas vulnérable ; référence non Intel /
ce système n'est pas vulnérable ; la version du microprogramme du moteur de gestion
n'est pas affectée /
ce système n'est pas vulnérable ; la référence du moteur de gestion n'est pas
affectée /
ce système n'est pas vulnérable ; le SMBIOS indique qu'il s'agit d'une référence
grand public /
ce système n'est pas vulnérable ; le système exécute le microprogramme SPS
(microprogramme de services de plate-forme serveur) /
Le microprogramme de ce système a été mis à jour et le système est hors service /
Le microprogramme de ce système a été mis à jour et le système est en service /
Consultez le constructeur /
```

```
le risque encouru par ce système est inconnu>

S'il est vulnérable, contactez votre constructeur pour obtenir de l'assistance et le
dépannage de ce système.

*** Pour plus d'informations ***
Reportez-vous au CVE-2017-5689 à :
     https://nvd.nist.gov/vuln/detail/CVE-2017-5689

Ou à l'avis de sécurité Intel Intel-SA-00075 à :
     https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-
00075&languageid=en-fr
```

La logique qui permet de réaliser une évaluation des risques est décrite dans Tableau 2.

Tableau 2. Signification de l'évaluation des risques dans le résultat

Message	Signification
Vulnérable	La version détectée du microprogramme du moteur de gestion est considérée comme vulnérable à INTEL-SA-00075.
Non vulnérable	Le système satisfait aux critères de non vulnérabilité décrits dans *Identifier les systèmes affectés à l'aide de l'outil* de détection INTEL-SA-00075, page 8.
Le microprogramme de ce système a été mis à jour et le système est hors service	Le microprogramme détecté sur ce système possède le correctif d'INTEL-SA-00075. Assurez-vous que les outils INTEL-SA-00075 ont été utilisés pour annuler la mise en service du système avant une remise en service. Cette opération supprimera tous les paramètres de configuration non autorisés.
Le microprogramme de ce système a été mis à jour et le système est en service	Le microprogramme détecté sur ce système possède le correctif d'INTEL-SA-00075. Si le système a été mis en service avant la mise à jour du microprogramme, un mise hors service complète et une remise en service du système supprimeront tous les paramètres de configuration non autorisés.
Consultez le constructeur	Les informations détectées dans le SMBIOS du constructeur indiquent la présence d'un produit d'administration, mais l'outil n'a pas reçu de réponse de votre ordinateur lorsqu'il a demandé des données détaillées. Cela peut être dû à l'absence du pilote d'interface du moteur de gestion. Consultez votre constructeur pour savoir si votre modèle d'ordinateur est concerné.
Inconnue	L'outil n'a pas reçu de réponse valide de votre ordinateur lors de la demande de données d'inventaire du matériel. Contactez le constructeur de votre système pour obtenir de l'aide concernant la vulnérabilité de ce système. Ce message peut-être être reçu sur une plate-forme serveur sur laquelle aucun pilote PMX n'est installé. Il est possible que ce pilote ne soit pas disponible sur toutes les versions du système d'exploitation Windows. Si le pilote n'est pas présent, la solution de contournement recommandée consiste à exécuter l'application spsInfo ou spsManuf fournie avec la version du microprogramme SPS. Ces applications installent toutes les deux le pilote PMX.

Résultats

Remarque : la quantité de données renvoyée par la commande discover d'INTEL-SA-00075 est différente si la pile du pilote d'administration Intel est chargée sur le système. Si le pilote de l'interface du moteur de gestion Intel® (MEI) et le service d'administration local (LMS) de l'application d'administration et de sécurité Intel® sont présents, l'ensemble de données renvoyé sera plus détaillé. Il est possible que certains champs ne soient pas pris en charge par le constructeur.

Emplacement dans le registre

Les valeurs du tableau de résultats se trouvent dans la clé de registre suivante :

- Systèmes d'exploitation 32 bits :`HKLM\SOFTWARE\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool`
- Systèmes d'exploitation 64 bits : `HKLM\SOFTWARE\WOW6432Node\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool`

XML

Si vous choisissez d'écrire les résultats dans un fichier XML, ce fichier sera stocké dans le répertoire dans lequel INTEL-SA-00075-console.exe est exécuté ou en suivant le chemin d'accès indiqué dans les options de ligne de commande. Les informations telles que l'inventaire du matériel, le système d'exploitation, la présence du service LMS, sont incluses. Si la technologie d'administration active est présente, la liste des hachages de certificats par défaut et personnalisés trouvés sera incluse. Cette liste peut être utilisée pour comparer les hachages attendus à ce qui est stocké dans la technologie d'administration active.

Codes de retour de console

Tableau 3. Codes de retour de la console INTEL-SA-00075

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

Tableau 4. Valeurs de sortie de la console INTEL-SA-00075

Valeur	Emplacement	Description
Application Version (Version de l'application)		La version de l'outil d'analyse utilisé
Scan Date (Date d'analyse)		Date et heure de l'analyse
Computer Name (Nom de l'ordinateur)		Le nom de l'ordinateur analysé
Computer Manufacturer (Constructeur de l'ordinateur)	Inventaire du matériel	Le nom du constructeur de l'ordinateur

Computer Model (Modèle de l'ordinateur)		Le modèle de l'ordinateur
Processor (Processeur)		Le modèle du processeur de l'ordinateur
ME Version (Version du moteur de gestion)	Informations sur le microprogramme du moteur de gestion	Une chaîne de valeur contenant le numéro de version du microprogramme du moteur de gestion dans le format suivant : Majeur.Mineur.Correctif.Build
ME SKU (Référence du moteur de gestion)		Si elle est présente, la fonction d'administration du système
ME Provisioning State (État de mise en service du moteur de gestion)		L'état de la configuration du moteur de gestion Aucun détecté Pas en service Mise en service en cours En service
ME Driver Installed (Pilote du moteur de gestion installé)		Valeur vrai/faux si le pilote de l'interface du moteur de gestion est présent sur l'ordinateur
EHBC Enabled (EHBC activé)		Valeur vrai/faux si le système est capable d'utiliser la méthode de mise en service utilisant une configuration basée sur l'hôte
LMS state (État LMS)		Informations indiquant si le service LMS est en cours d'exécution, pas en cours d'exécution ou absent
LMS startup type (Type de démarrage LMS)		Informations indiquant si le type de démarrage LMS est Absent, Démarrage, Système, Automatique, Manuel ou Désactivé
MicroLMS state (État MicroLMS)		Informations indiquant si le service MicroLMS est en cours d'exécution, pas en cours d'exécution ou absent
MicroLMS startup type (Type de démarrage MicroLMS)		Informations indiquant si le type de démarrage MicroLMS est NotPresent (absent), Boot (démarrage), System (système), Auto (automatique), Manual (manuel) ou Disabled (désactivé)
Control Mode (Mode de contrôle)		Le mode de configuration du moteur de gestion None (Aucun), ACM ou CCM
Is CCM Disabled (CCM est désactivé)		État True/False/Unknown (Vrai/Faux/Inconnu) de la désactivation du mode de contrôle client (CCM)
Is SPS (Est SPS)		La plate-forme est-elle un système SPS (Server Platform Services) non vulnérable ?
*** Évaluation des risques ***	Évaluation des risques	Voir *Tableau 2. Signification de l'évaluation des risques dans le résultat*

Identifier les systèmes affectés à l'aide de l'outil de détection INTEL-SA-00075

Les systèmes affectés sont définis comme possédant une version du microprogramme du moteur de gestion Intel® affectée et contenant un des trois ensembles de fonctionnalités d'administration, comme définis dans Tableau 5.

Remarque : les plates-formes Server Platform Services (SPS) ne sont pas vulnérables à INTEL-SA-00075. Le microprogramme des plates-formes SPS est exécuté sur le moteur de gestion (ME) (partie des PCH) sur les plates-formes serveur. Ce microprogramme est différent du microprogramme d'administration Intel (également exécuté sur le moteur de gestion) des PC et stations de travail.

Tableau 5. Critères permettant de déterminer si un système est vulnérable à INTEL-SA-00075 à l'aide de l'outil de détection INTEL-SA-00075

Nom de la valeur	Vulnérable	Non vulnérable
`Référence du moteur de gestion`	Administration complète par la technologie d'administration active Intel® Module Intel® Standard Manageability Intel® Small Business Advantage	Les valeurs de la référence du moteur de gestion ne figurent pas dans la liste des produits vulnérables à gauche – OU – Valeurs de la référence du moteur de gestion à gauche avec une version de microprogramme qui n'est pas vulnérable

Version du moteur de gestion	Moteur de gestion de version 6.x.x.x – 11.7.x.x avec une valeur de build de moins de 3000 Exemple : 9.5.22.**1760**	Versions du moteur de gestion : • 6.x.x.x – 11.7.x.x avec une valeur de build supérieure ou égale à 3000 o Exemple : 11.6.27.**3264** • 2.x.x.x. – 5.x.x.x • 11.7.x.x ou supérieure

Remarque : la technologie Intel® SBT (Small Business Technology) est le produit d'administration d'Intel® Small Business Advantage (SBA).

Extension de l'inventaire du matériel Microsoft* SCCM pour inclure les résultats de l'outil de la console INTEL-SA-00075

Si vous choisissez de stocker les résultats de l'outil de la console Intel-SA-00075 dans le registre de Windows, vous pouvez exploiter l'extensibilité de l'inventaire du matériel de Microsoft* SCCM pour importer les résultats. Cela vous permettra d'accumuler des collections dans SCCM pour cibler des ordinateurs pour le dépannage et la mise à jour du microprogramme. Pour ce faire, vous devrez procéder comme suit :

1. Ajoutez des classes d'inventaire de matériel au fichier SCCM configuration.mof.
2. Activez ces nouvelles classes d'inventaire de matériel lors de la configuration du client.
3. Créez un package de logiciels pour déployer et exécuter l'outil de la console INTEL-SA-00075 (`Intel-SA-00075-console.exe`).
4. Créez une séquence de tâches pour exécuter le package de logiciels.

Modification d'un fichier MOF

Remarque : si votre environnement possède un serveur central, modifiez le fichier MOF dessus. Sinon, effectuez ces modifications sur chacun de vos serveurs principaux.

1. Localisez votre fichier configuration.mof. Il se trouve généralement dans \Program Files\Microsoft Configuration Manager\inboxex\clifiles.src\hinv\
2. Faites une copie de sauvegarde.
3. Modifiez le fichier configuration.mof, en faisant défiler le texte jusqu'à la fin et en plaçant le curseur au-dessus de cette ligne :

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

4. Collez le contenu des modifications du fichier MOF des pages 13-14 de ce document au-dessus de la ligne de l'étape trois.
5. Enregistrez et fermez le fichier.
6. Lancez une invite de commande en tant qu'administrateur dans le répertoire contenant le fichier configuration.mof.
7. Exécutez mofcomp sans commutateurs en ciblant le fichier configuration.mof modifié.

Modification de l'inventaire de matériel

Remarque : une fois réalisées, ces modifications prendront du temps à se propager à vos clients avant que ces nouveaux éléments s'affichent dans l'inventaire du matériel. La durée de cette opération varie en fonction de la configuration de votre environnement.

1. Créez un nouveau fichier appelé INTEL-SA-00075.mof.
2. Collez le contenu de la section Importation de l'inventaire matériel INTEL-SA-00075, page 175 dans le fichier nouvellement créé et enregistrez-le.
3. Lancez la console du Gestionnaire de configuration.
4. Administration > Paramètres des clients > Paramètres par défaut des clients.
5. Cliquez avec le bouton droit sur Paramètres par défaut des clients > Propriétés.
6. Sélectionnez Inventaire matériel > Définir des classes.
7. Cliquez sur Importer.
8. Naviguez jusqu'au fichier INTEL-SA-00075.mof > Ouvrir.
9. Vérifiez que l'option « Importer classes d'inventaire matériel et paramètres de classe d'inventaire matériel » est sélectionnée.
10. Cliquez sur Importer.
11. OK > OK.
12. SCCM enregistre les modifications apportées à l'inventaire du matériel dans le fichier dataldr.log.

Créer un package SCCM

1. Créez le fichier de commandes à partir de la page 15 et placez-le dans un dossier avec le fichier de l'outil de la console INTEL-SA-00075.
2. Lancez la console du Gestionnaire de configuration.
3. Bibliothèque de logiciels > Packages.
4. Cliquez avec le boutont droit sur Packages > Créer le package.
5. Nom : Intel-SA-00075
6. Vérifiez que ce package contient les fichiers source.
7. Accédez au dossier du package de la première étape.
8. Suivant.
9. Sélectionnez Ne pas créer de programme.
10. Suivant > Suivant > Fermer.
11. Distribuez le package aux points de distribution appropriés.

Créer une séquence de tâches SCCM

1. Lancez la console du Gestionnaire de configuration.
2. Bibliothèque de logiciels > Systèmes d'exploitation.
3. Cliquez avec le bouton droit sur Séquences de tâches > Créer une séquence de tâches.
4. Sélectionnez Créez une séquence de tâches personnalisée.
5. Suivant.
6. Entrez le nom Intel-SA-00075.

7. Suivant > Suivant > Fermer.
8. Cliquez avec le bouton droit sur la séquence de tâches Intel-SA-00075 et cliquez sur Modifier.
9. Ajouter > Général > Exécuter la ligne de commande.
10. Entrez Intel-SA-00075.bat dans le champ de ligne de commande.
11. Cochez la case Package et cliquez sur Parcourir.
12. Sélectionnez le package Intel-SA-00075 précédemment créé > OK.
13. Cliquez sur OK.

Utilisation de l'utilitaire de découverte de système Intel® SCS

Qu'est-ce que l'utilitaire de découverte de système Intel® SCS ?

L'utilitaire de découverte de système Intel® SCS est un composant de la suite Intel® Setup and Configuration Software (Intel® SCS) qui fournit des détails spécifiques sur le matériel et les logiciels d'un système prenant en charge la technologie d'administration active Intel®, Intel® Standard Manageability (ISM) ou Intel® Small Business Technology (Intel® SBT). Lorsqu'il est exécuté, il peut enregistrer les résultats dans le registre Microsoft Windows ou dans un fichier XML. Ces informations peuvent être utilisées pour rechercher des systèmes pour cibler les mises à jour de microprogrammes ou mettre en œuvre des mesures d'atténuation des risques.

Obtenir l'utilitaire de découverte de système Intel® SCS

Le package de téléchargement de l'utilitaire de découverte de système Intel® SCS est disponible à https://downloadcenter.intel.com/fr/download/26691/Intel-SCS-System-Discovery-Utility.

Déterminer la version du microprogramme d'administration à l'aide de l'utilitaire de découverte de système Intel® SCS

La sortie de l'utilitaire de découverte de système Intel® SCS peut servir à déterminer la version du microprogramme d'un système et si le système est un produit d'administration. Ces informations sont fournies dans la section `ManageabilityInfo` de la sortie. Pour obtenir des instructions sur l'exécution de l'outil, consultez la section *Exécuter l'utilitaire de découverte de système Intel® SCS*, page 12.

La valeur de `FWVersion` contient la version du microprogramme actuellement sur l'ordinateur. La valeur `AMTSSKU` contient les produits d'administration pris en charge, le cas échéant. Examinez les valeurs de `FWVersion` et d'`AMTSKU` pour déterminer les vulnérabilités de votre système comme décrit dans Tableau 6.

Tableau 6. Critères permettant de déterminer si un système est vulnérable à INTEL-SA-00075 à l'aide de l'outil de découverte de système Intel® SCS

Nom de la valeur	Vulnérable	Non vulnérable
`AMTSKU`	Administration complète par la technologie d'administration active Intel (R) Administration standard Intel (R) Intel(R) Small Business Advantage Exemple de sortie :	La valeur AMTSKU ne se trouve pas dans la sortie – OU – Valeurs AMTSKU à gauche avec une version de microprogramme qui n'est pas vulnérable Exemple de sortie : <ManageabilityInfo> <FWVersion>**9.0.13.1402**</FWVersion>

	<ManageabilityInfo> <AMTSKU>Intel(R) Full AMT Manageability</AMTSKU> <AMTversion>11.0.0</AMTversion> <FWVersion>11.0.0.1202</FWVersion>	
FWVersion	Microprogramme du produit d'administration Intel® versions 6.x.x.x – 11.7.x.x avec une valeur de build inférieure à 3000 Exemple : 9.5.22.**1760**	Microprogramme de produit d'administration Intel® versions : • 6.x.x.x – 11.7.x.x avec une valeur de build supérieure ou égale à 3000 o Exemple : 11.6.27.**3264** • 2.x.x.x. – 5.x.x.x • 11.7.x.x ou supérieure

Remarque : la technologie Intel® SBT (Small Business Technology) est le produit d'administration d'Intel® Small Business Advantage (SBA).

Exécuter l'utilitaire de découverte de système Intel® SCS

Enregistrer les données dans le registre uniquement

Exécutez la commande suivante en tant qu'administrateur depuis une invite de commande pour exécuter l'utilitaire de découverte de système Intel® SCS et écrire les données dans le registre :

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

Enregistrer les données dans un fichier XML uniquement

Utilisez la commande suivante pour exécuter l'utilitaire de découverte de système Intel® SCS et enregistrer les données dans un fichier XML :

```
SCSDiscovery.exe SystemDiscovery <nom du fichier et chemin d'accès> /noregistry
```

Le nom du fichier et le chemin d'accès peuvent être un emplacement local sur le système ou un partage réseau. Si vous choisissez d'utiliser un partage réseau, assurez-vous que le compte exécutant l'utilitaire de découverte de système Intel® SCS dispose d'autorisations d'écriture sur ce partage réseau. Si vous ne spécifiez pas de nom de fichier et de chemin d'accès, le nom de domaine complet (FQDN) du système sera utilisé pour le nom du fichier XML et le fichier sera stocké dans le répertoire qui contient l'utilitaire de découverte de système Intel® SCS.

Enregistrer les données dans le registre et un fichier XML

Utilisez la commande suivante pour exécuter l'utilitaire de découverte de système Intel® SCS et enregistrer les données dans le registre et un fichier XML

```
SCSDiscovery.exe SystemDiscovery <nom du fichieri et chemin d'accès>
```

Comme dans l'exemple précédent, si vous ne spécifiez pas de nom de fichier et de chemin d'accès, le nom de domaine complet (FQDN) du système sera utilisé pour le nom du fichier XML et le fichier sera stocké dans le répertoire qui contient l'utilitaire de découverte de système Intel® SCS.

Résultats de l'utilitaire de découverte de système Intel® SCS

La quantité de données renvoyée par l'utilitaire de découverte de système Intel® SCS est différente si la pile du pilote d'administration Intel est chargée sur le système. Si le pilote de l'interface du moteur de gestion Intel® (MEI) et le service d'administration local (LMS) de l'application d'administration et de sécurité Intel® sont présents, l'ensemble de données renvoyé sera plus détaillé. Les résultats décrits ci-dessous se concentrent sur quelques champs de données clés liés au problème d'escalade des privilèges connu. Pour davantage d'informations sur les autres champs de données, reportez-vous à la documentation de l'utilitaire de découverte de système Intel® SCS. Il est possible que certains champs ne soient pas pris en charge par le constructeur.

Résultats du registre

Les résultats enregistrés dans le registre se trouvent à l'emplacement suivant :
`HKLM\Software\Intel\Setup and Configuration Software\SystemDiscovery`

Valeurs de clé :

Nom de la valeur	Sous-clé de registre	Description de la valeur
FWVersion	ManageabilityInfo	Version du microprogramme du moteur de gestion Intel®
AMTSKU	ManageabilityInfo	Fonctionnalité d'administration prise en charge, le cas échéant

Résultats du fichier XML

La version du microprogramme du moteur de gestion Intel® se trouve dans le chemin d'accès suivant dans le fichier XML :

```
<SystemDiscovery>
       <ManageabilityInfo>
              <FWVersion> Numéro de version </FWVersion>
```

La fonctionnalité d'administration prise en charge par le système, le cas échéant, se trouve dans le chemin d'accès suivant du fichier XML :

```
<SystemDiscovery>
       <ManageabilityInfo>
              <AMTSKU> Nom de la fonctionnalité d'dministration </AMTSKU>
```

Importer les données de découverte de système dans l'inventaire de matériel SCCM

Le processus de collecte des données de découverte de système peuvent être automatisé avec le module d'extension Intel® SCS pour Microsoft* System Center Configuration Manager (SCCM). Lorsqu'il est installé, ce module d'extension étend automatiquement l'inventaire matériel SCCM pour inclure des données de découverte de système et créer des séquences de tâches qui peuvent être utilisées pour exécuter la découverte de système sur des groupes de systèmes. Les informations recueillies par ce processus peucent ensuite être utilisées pour créer des collections SCCM pour la mise à jour de microprogramme ou l'atténuation des risques sur des systèmes affectés.

La package de téléchargement du module d'extension Intel® SCS pour Microsoft SCCM est disponible à https://downloadcenter.intel.com/fr/download/26506/Intel-SCS-Add-on-for-Microsoft-System-Center-Configuration-Manager.

Modifications du fichier 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 ====
```

Importation de l'inventaire matériel 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;
};
```

Fichier de commandes 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%
```

Exemples de requêtes de collecte

Ordinateursmis à disposition

```
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 en cours d'exécution

```
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"
```