

Guida alla rilevazione e mitigazione di 00075-INTEL-SA

Tecnologia Intel® Active Management, Intel® Standard Manageability (ISM) e tecnologia Intel® Small Business

Istruzioni per il rilevamento e la mitigazione di NTEL-SA-00075

Revisione 1.3 - giovedì 20 luglio 2017

Introduzione

Questo documento guiderà l'utente attraverso più processi per rilevare e ridurre la vulnerabilità della sicurezza descritta nell'amministratore di sistema-SA -INTEL-00075. Per ulteriori informazioni, leggere l'avviso pubblico sulla sicurezza <https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr>.

Se si è un utente di un singolo PC e si desidera determinarne lo stato: forniamo l'applicazione INTEL-SA-00075 Discovery GUI per l'analisi locale di un sistema singolo o standalone.

Se si desidera determinare lo stato e/o di applicare la riduzione dei rischi per più computer: abbiamo messo a disposizione i meccanismi di rilevamento di INTEL-SA-00075 e l'applicazione della console strumento di riduzione rischi (Intel-SA-00075-console.exe). Questo strumento può eseguire il rilevamento e scrivere i risultati della ricerca nel Registro di sistema locale di Windows e, in modo facoltativo, in un file XML, per le successive raccolta e analisi. L'applicazione console può anche aiutare a implementare la riduzione dei rischi. Vedere *Uso dello strumento di mitigazione e rilevamento* di INTEL-SA-00075 a pagina 2 per altre informazioni.

Se l'utente è un amministratore di rete che sta già utilizzando il software Intel® per configurazione e installazione (Intel® SCS): la Suite Intel® SCS contiene uno strumento console alternativo, l'utility Intel® SCS. System Discovery Si consiglia di utilizzare questo strumento se si ha già familiarità con gli strumenti di Intel® SCS o si desidera ottenere dati dettagliati sulla tecnologia Intel® Active Management. Vedere *Utilizzo dell'utility System Discovery di Intel® SCS* a pagina 121.

Mitigazione

I passaggi per la mitigazione descritti in questo documento sono stati concepiti per evitare l'attivazione e l'utilizzo non autorizzati di SKU di gestibilità di Intel, tecnologia Intel® Active Management, Intel® Standard Manageability (ISM) e tecnologia Intel® Small Business a cui non sono stati applicati gli aggiornamenti del firmware che risolvono la vulnerabilità.

I professionisti IT possono utilizzare queste istruzioni come base per gli script o le attività all'interno delle console di gestione al fine di eseguire implementazioni su larga scala delle procedure di mitigazione. La procedura per implementare la mitigazione è la seguente:

1. Annullamento del provisioning dei client degli SKU di gestibilità di Intel per ridurre il rischio che malintenzionati senza privilegi attacchino la rete e acquisiscano privilegi di sistema
2. Disattivazione o rimozione di Local Manageability Service (LMS) per ridurre il rischio che malintenzionati locali senza privilegi acquisiscano privilegi di sistema
3. Configurazione opzionale di restrizioni alla configurazione della gestibilità locale

Intel raccomanda che il primo passo di tutte le procedure di mitigazione sia annullare il provisioning degli SKU di gestibilità di Intel per risolvere la vulnerabilità privilege escalation della rete. Per i sistemi con provisioning, l'annullamento del provisioning deve essere eseguito prima di disattivare o rimuovere LMS. In attesa della disponibilità del firmware aggiornato degli SKU di gestibilità di Intel, Intel raccomanda di attenuare il problema di privilege escalation locale rimuovendo o disattivando LMS. Se si desidera avere un secondo livello di difesa dall'accidentale reinstallazione o riattivazione di LMS, è possibile anche disattivare dal sistema operativo alcune opzioni di configurazione della gestibilità eseguite tramite il sistema operativo. Tuttavia, l'annullamento di queste restrizioni aggiuntive alla configurazione della gestibilità locale è soggetto a vincoli.

Nota: l'AMT 6.0. x non supporta il modello di provisioning della base host/modello di controllo client; di conseguenza, non può restare senza provisioning mediante l'interfaccia di sistema operativo locale, tramite meccanismi di rilevamento di INTEL-amministratore di sistema-00075 e strumento di mitigazione. Per le piattaforme che usano il firmware di gestibilità 6.0. x. x o 6.1. x. x, sarà necessario annullare completamente il provisioning utilizzando la SCS Suite ACUConfig/completa Intel o i sistemi MEBx.

Per assistenza nell'implementazione dei passaggi di mitigazione forniti in questo documento, contattare il [Supporto clienti Intel](#). Nella sezione Tecnologie, selezionare la tecnologia Intel® Active Management.

Uso dello strumento di mitigazione e rilevamento di INTEL-SA-00075

Che cos'è lo strumento di rilevamento e mitigazione INTEL-SA-00075?

Lo strumento di rilevamento e mitigazione INTEL-SA-00075 Discovery Tool può essere utilizzato dagli utenti locali o da un amministratore IT per determinare se un sistema è vulnerabile agli attacchi documentati nell'avviso sulla sicurezza di Intel INTEL-SA-00075. La versione console dello strumento si può utilizzare per eseguire passaggi di operazioni di mitigazione.

Lo strumento di mitigazione e rilevamento viene offerto in due versioni.

- Il primo è uno strumento GUI interattivo che, quando eseguito, rileva le informazioni relative all'hardware e al software del dispositivo e offre un'indicazione della valutazione del rischio. Questa versione è consigliata quando si desidera una valutazione locale del sistema.
- La seconda versione è una console eseguibile che può eseguire la valutazione dei rischi e passaggi delle procedure di mitigazione consigliate. È possibile salvare le informazioni di individuazione può includere nel Registro di sistema Windows * e/o in un file XML. Questa versione è più pratica per gli amministratori IT, se si desidera eseguire le operazioni di rilevamento e la mitigazione in bulk tra più computer.

Come ottenere lo strumento di rilevamento e mitigazione INTEL-SA-00075

Il pacchetto di download dello strumento di rilevamento e mitigazione INTEL-SA-00075 è disponibile all'indirizzo: <https://www.intel.com/Content/www/it/it/support/Technologies/000024133.HTML>.

Requisiti di sistema

- Microsoft Windows* 7, 8, 8.1 o 10
- Accesso amministrativo al sistema operativo locale

Installazione del tool

Installazione interattiva

Eseguire lo strumento di rilevamento e mitigazione Tool.msi INTEL-SA-00075 e seguire le istruzioni che appaiono sullo schermo.

Installazione invisibile all'utente

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

Questo comando installerà lo strumento di rilevamento e mitigazione INTEL-SA-00075 nella directory predefinita, C:\Program Files (x86)\Intel\Intel-SA-00075 Detection and Mitigation Tool\

Disinstallazione del tool

Disinstallazione interattiva

Eseguire lo strumento di rilevamento e mitigazione Tool.msi INTEL-SA-00075 e seguire le istruzioni che appaiono sullo schermo.

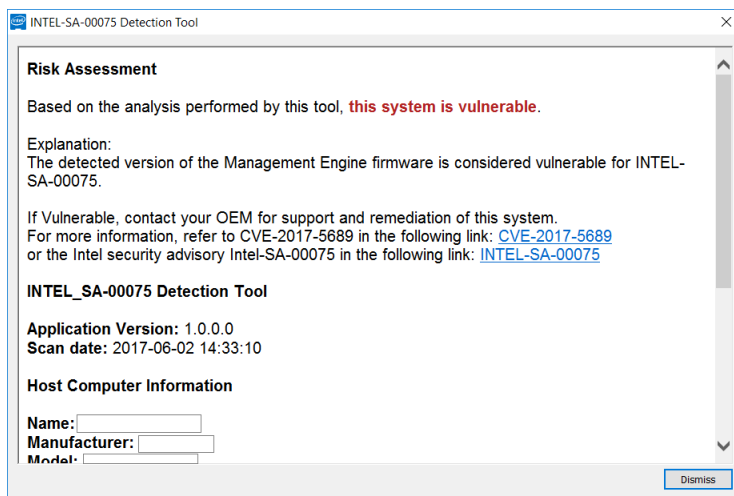
Disinstallazione invisibile all'utente

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

Esecuzione del tool GUI

INTEL-SA-00075-GUI.exe è progettato per funzionare su un unico sistema. Quando viene eseguito, il tool visualizza le informazioni di rilevamento sullo schermo.

Figura 1. Esempio dei risultati di INTEL-SA-00075-GUI visualizzati sullo schermo



Esecuzione del tool della console

Eseguire `INTEL-SA-00075-console.exe` da un prompt dei comandi con diritti amministrativi.

Utilizzo:

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

Solo un comando alla volta può essere eseguito. Se non viene specificato alcun comando, sarà eseguito il comando `discover`.

Tabella 1. Switch tasti della riga di comando della console INTEL-SA-00075

Riga di comando	Comando	Funzionalità
-Discover		Emette risultati per la console e scrivere i dati nel Registro di sistema.
-Unprovision [password], -u [password]		Rimuovere tutte le impostazioni di Intel AMT e disattivare le funzioni Intel AMT; si può utilizzare una password utente amministratore per il dispositivo Intel AMT e potrebbe essere obbligatoria. Nota: questo comando richiamato senza una password funziona solo con le versioni del firmware legata a INTEL-SA-00075 (6.1. x. x-11.6. x. x con un numero di build inferiore a 3000). Se si utilizza il firmware versioni 6.1.x.x-11.6. X.x.x con un numero di build superiore a 3000, il provisioning funzionerà solo se viene fornita una password.
-DisableClientControlMode, -DisableCCM		Disattiva in modo permanente l'opzione modalità Controllo client del dispositivo Intel AMT. Dopo avere eseguito questo comando, il dispositivo non può essere messo in modalità di Controllo client. Nota: nessun comando CLI può annullare questa azione. Avviso: non tutte le piattaforme possono abilitare nuovamente la modalità CCM una volta disattivata.
-DisableLMS		Disabilita il servizio LMS.

Opzione della riga di comando	Funzionalità
-n, --noregistry	Impedisce la scrittura dei risultati nel Registro di sistema
-c, --noconsole	Impedisce la visualizzazione dei risultati sulla console
-d, - delay < seconds >	Ritardo in secondi prima di iniziare l'esecuzione. Se nessun valore viene specificato, lo strumento non disporrà di alcun ritardo.
-f, --writefile	Specifica di scrivere i risultati in un file. Il nome del file utilizza il seguente formato: <nomecomputer>_System_Summary.xml
-p, --filepath -filepath < filepath >	Il percorso dove memorizzare il file di output. Se non viene specificato alcun percorso, il file verrà scritto nella directory da cui viene eseguito il tool.
-h, --help	Consente di visualizzare queste opzioni della riga di comando e le relative funzioni

-Discover

Il comando `discover` emette informazioni di rilevamento nella console. Per impostazione predefinita scrive anche i dati di rilevamento nel Registro di sistema. Se nessun comando viene fornito per il tool di console, viene eseguito il comando `discover`.

-Annulla provisioning

Rimuovere tutte le impostazioni di Intel AMT e disattivare le funzioni Intel AMT, si può utilizzare una password utente amministratore opzionale per il dispositivo Intel AMT.

Quando sono configurati, la tecnologia Intel® Active Management e ISM automaticamente rilevano il traffico di gestione sulla rete di computer. Per i sistemi vulnerabili al noto problema di escalation privilegi, il provisioning deve essere annullato utilizzando il comando Annulla provisioning per impedire l'accesso non autorizzato alle funzioni di gestibilità.

Richiamare questo comando senza una password funziona solo con le versioni del firmware condizionate da INTEL-SA-00075 (6.1. x.x–11.6. x.x con un numero di build inferiore a 3000). Se si utilizza il firmware versioni 6.1.x.x–11.6. X.x.x con un numero di build superiore a 3000, il provisioning funzionerà solo se viene fornita una password.

-DisableClientControlMode

La limitazione di configurazione DisableClientControlMode rappresenta un passo opzionale per i clienti che richiedono un livello secondario per proteggersi da un annullamento della mitigazione da parte di un utente malintenzionato senza privilegi, che ha guadagnato privilegi di amministratore di sistema operativo. L'annullamento di queste opzioni è difficile, potrebbe non essere supportato dal produttore del computer e potrebbe richiedere l'accesso fisico al sistema. Se si sceglie di eseguire questa ulteriore restrizione della configurazione, si deve eseguirla prima di disattivare il servizio LMS.

Passaggi per riattivare CCM

Se quest'azione è supportata dal produttore, è possibile reimpostare gli SKU di gestibilità Intel dal BIOS, riattivando così CCM. Consultare il produttore per vedere se questa funzionalità è supportata e per sapere la procedura da seguire.

Nota: il produttore potrebbe fornire strumenti che consentono di configurare le impostazioni del BIOS tramite il sistema operativo. Questi strumenti, se disponibili, potrebbero consentire di reimpostare gli SKU di gestibilità di Intel nel BIOS senza dover fisicamente intervenire sul computer. Consultare il produttore per verificare se è disponibile uno strumento con questa funzionalità.

-DisableLMS

Il comando DisableLMS disabilita il servizio LMS come fase di mitigazione.

Cos'è LMS?

Local Management Service (LMS) dell'applicazione Intel® Management and Security è un servizio che consente alle applicazioni locali in esecuzione su dispositivi supportati dalla tecnologia Intel® Active Management, Intel® Small Business Advantage o Intel® Standard Manageability di utilizzare le funzionalità comuni di SOAP e WS-Management. Ascolta le porte del motore di gestione Intel® (16992, 16993, 16994, 16995, 623 e 664) e indirizza il traffico al firmware tramite il driver dell'interfaccia del motore di gestione Intel®.

Considerazioni aggiuntive

Tutti gli utenti con i privilegi amministrativi del sistema operativo saranno in grado di reinstallare LMS se è stato rimosso o di riattivare il servizio se è stato disattivato. Di conseguenza, è importante prestare la massima cautela per evitare che l'LMS sia accidentalmente reinstallato o riattivato mentre nel sistema è presente la vulnerabilità. Ad esempio, LMS potrebbe essere reinstallato se in futuro si dovesse eseguire il programma di installazione del software di gestibilità di Intel.

Figura 2 Esempio dell'output della console INTEL-SA-00075

```
INTEL-SA-00075 Discovery Tool
Versione applicazione: <versione applicazione>
Data scansione: <data e ora>

*** Informazioni sul computer host ***
Nome computer: <nome computer>
Produttore: <produttore computer>
Modello: <modello computer>
Processore: <modello processore>
Versione Windows: <versione Windows*>

*** Informazioni sul motore di gestione ***
Versione: <versione firmware motore di gestione Intel>
```

```

SKU: <funzione di gestibilità, se ne è presente una>
Stato: <stato di provisioning motore di gestione>
Driver installati: <True/False>
Modalità di controllo: <Nessuna/ACM/CCM>
CCM è disattivato: <True/False/Sconosciuto>
EHBC attivato: <True/False>
Stato LMS: <In esecuzione/Interrotto/Non presente>
LMS startup type: <Boot/System/Auto/Manuel/Disabled/NotPresent>
Stato MicroLMS: <In esecuzione/Interrotto/Non presente>
Tipo di avvio MicroLMS: <Boot/System/Auto/Manuel/Disabled/NotPresent >
È SPS: <True/False>

*** Valutazione del rischio ***
Basato sull'analisi eseguita con questo strumento,
<questo sistema è vulnerabile /
questo sistema non è vulnerabile /
questo sistema non è vulnerabile; SKU non -Intel /
questo sistema non è vulnerabile; la versione del firmware ME non è interessata dal
problema /
questo sistema non è vulnerabile; la SKU ME non è interessata dal problema /
questo sistema non è vulnerabile; il SMBIOS indica che si tratta di un consumatore
SKU /
questo sistema non è vulnerabile; il sistema è in esecuzione FW SPS (Firmware
Servizi della piattaforma Server) /
è stato aggiornato il Firmware di questo sistema e il sistema è in stato di un-
provisioning /
è stato aggiornato il Firmware di questo sistema e il sistema è in stato di
provisioning /
Controllare con OEM.
il rischio di questo sistema è sconosciuto >

Se Vulnerable, contattare l'OEM per il supporto e la riparazione del sistema.

*** Per ulteriori informazioni ***
Fare riferimento a CVE-2017-5689:
    https://nvd.nist.gov/vuln/detail/CVE-2017-5689

o all'avviso sulla sicurezza di Intel Intel-SA-00075:
    https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-
00075&languageid=en-fr

```

La logica usata per determinare una valutazione dei rischi è descritta in Tabella2.

Tabella2. Significato della valutazione del rischio nell'output

Messaggio	Significato
Vulnerabile	La versione del firmware del motore di gestione rilevata è considerata vulnerabile per INTEL-SA-00075.
Non vulnerabile	Il sistema soddisfa i criteri di "Non vulnerabilità" descritti in <i>Identificazione dei sistemi interessati utilizzando INTEL-SA-00075 Discovery Tool</i> a pagina 8.
È stato aggiornato il firmware di questo sistema, che è in stato di un-provisioning	Il firmware rilevato nel sistema in uso ha la correzione necessaria per INTEL-SA-00075. Verificare che gli strumenti di INTEL-SA-00075 siano stati utilizzati per eseguire un completo annullamento del provisioning di sistema prima del nuovo provisioning. Verranno rimosse le impostazioni di configurazione non autorizzati.

Messaggio	Significato
È stato aggiornato il Firmware di questo sistema, che è in stato di provisioning	Il firmware rilevato nel sistema in uso ha la correzione necessaria per INTEL-SA-00075. Se il sistema è stato effettuato il provisioning prima l'aggiornamento del firmware, una completa annullamento del provisioning e nuova provision del sistema verranno rimossi le impostazioni di configurazione non autorizzati.
Check with OEM	Check With OEM: le informazioni nell'SMBIOS dell'OEM mostrano uno SKU di gestibilità, ma il Discovery Tool non ha ricevuto una risposta quando ha richiesto dati dettagliati al computer. Questa situazione potrebbe essere causata dalla mancanza di un driver dell'interfaccia del motore di gestione. Consultare l'OEM per sapere se il modello di computer è interessato dal problema.
Sconosciute	<p>Sconosciute: lo strumento Tool non ha ricevuto una risposta valida quando ha richiesto dati relativi all'inventario hardware del computer. Per l'assistenza nel determinare la vulnerabilità di questo sistema, contattare il produttore del sistema.</p> <p>Questo messaggio potrebbe essere ricevuto su una piattaforma server senza un Driver PMX installato. Questo driver potrebbe non essere disponibile in tutte le versioni del sistema operativo Windows. Se il driver non è presente, la soluzione consigliata è quella di eseguire l'applicazione spsInfo o spsManuf dotata della versione del Firmware SPS. Entrambe le applicazioni installeranno il Driver PMX.</p>

Risultati

Nota: la quantità di dati restituiti dal comando INTEL-SA-00075 Discover dipenderà dal caricamento nel sistema dello stack di driver di gestibilità Intel. Se sono presenti il driver dell'interfaccia del motore di gestione Intel® e Local Management Service (LMS) dell'applicazione Intel® Management and Security, il set di dati disponibile sarà più dettagliato. Alcuni campi potrebbero non essere supportati dal produttore.

Percorso del Registro di sistema

I valori della tabella dei risultati si trovano nella seguente chiave del Registro di sistema:

- sistemi operativi a 32 bit: HKLM\SOFTWARE\HKLM\SOFTWARE\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool
- sistemi operativi a 64 bit: HKLM\SOFTWARE\WOW6432Node\HKLM\SOFTWARE\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool

XML

Se si sceglie di scrivere i risultati in un file XML, il file sarà archiviato nella directory da cui viene eseguito INTEL-SA-00075-console.exe o nel percorso specificato nelle opzioni della riga di comando. In informazioni quali hardware, sistema operativo, la presenza LMS è inclusa. Se AMT è presente, l'elenco degli hash predefiniti e dei certificati personalizzati trovati verranno inclusi. Questo elenco potrebbe essere utilizzato per controllare hash a fronte di quello che è memorizzato AMT.

Codici di ritorno console

Tabella 3. Codici di ritorno console INTEL-SA-00075

Numero	Significato
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

Tabella 4 Valori di output della console INTEL-SA-00075

Valore	Ubicazione	Descrizione
Application Version (Versione applicazione)		La versione del tool di scansione utilizzato
Scan Date (Data di scansione)		Data e ora in cui è stata eseguita la scansione
Computer Name (Nome computer)		Il nome del computer scansionato
Computer Name (Produttore del computer)	Inventario hardware	Il produttore del computer
Computer Model (Modello di computer)		Il modello del computer
Processor (Processore)		Modello del processore del computer
ME Version (Versione ME)	Informazioni firmware motore di gestione	Un valore stringa con il numero di versione completo del firmware del motore di gestione nel seguente formato: Major.Minor.Hotfix.Build
ME SKU (SKU ME)		Se è presente, la funzione di gestibilità di cui è dotato il sistema
ME Provisioning State (Stato di provisioning ME)		Lo stato di configurazione del motore di gestione Nessuno rilevato Nessun provisioning Provisioning in corso Provisioning effettuato
ME Driver Installed (Driver ME installato)		Valore True/False se il driver dell'interfaccia del motore di gestione è presente nel computer
EHBC Enabled (EHBC Attivato)		Valore True/False se il sistema è compatibile con il metodo di provisioning Embedded Host Based Configuration
LMS state (Stato del servizio LMS)		Informazioni se il servizio LMS è in esecuzione, non in esecuzione o non presente
LMS startup type (Tipo di avvio del servizio LMS)		Informazioni riguardo il tipo di avvio del sistema LMS: Non Presente, Avvio, Sistema, Auto, Manuale o Disattivato
MicroLMS state (Stato di MicroLMS)		Informazioni riguardo il servizio Micro LMS: è in esecuzione, non in esecuzione o non presente
MicroLMS startup type (Tipo di avvio MicroLMS)		Informazioni sul tipo di avvio MicroLMS: Non Presente, Avvio, Sistema, Auto, Manuale o Disattivato
Control Mode (Modalità controllo)		La modalità di configurazione del motore di gestione Nessuna, ACM o CCM
Is CCM Disabled (CCM è disattivato?)		Stato True/False/Unknown per la modalità di controllo client è disattivata
Is SPS (È SPS)		La piattaforma di un sistema di Servizi di piattaforma Server (SPS) non è

		vulnerabile?
*** Valutazione del rischio ***	Valutazione dei rischi	Vedere Tabella2 . Significateo della valutazione del rischio nell'output

Identificazione dei sistemi interessati utilizzando INTEL-SA-00075 Discovery Tool

I sistemi interessati sono definiti in questo modo: hanno una versione di firmware Intel® Management Engine (ME) e contengono uno dei tre gruppi di funzioni di gestibilità come definiti in Tabella 5.

Nota: le piattaforme server Servizi di piattaforma (SPS) non sono vulnerabili rispetto a INTEL-SA-00075. Le piattaforme SPS sono firmware in esecuzione su Manageability Engine (ME) (parte della PCH) su piattaforme server. Questo firmware è diverso da quello del firmware di gestibilità Intel (anche in esecuzione su di ME) su piattaforme PC e Workstation.

Tabella 5. Criteri per determinare se un sistema è vulnerabile agli INTEL-SA-00075 utilizzando lo strumento di rilevamento di INTEL-SA-00075

Nome valore	Vulnerabile	Non vulnerabile
SKU ME	Intel® Full AMT Manageability Intel® Standard Manageability Intel® Small Business Advantage	I valori ME SKU non presenti nell'elenco delle funzionalità vulnerabili a sinistra -oppure- I valori ME SKU a sinistra con una versione del firmware che non è vulnerabile
Versione ME	Versioni ME del motore di gestione 6.x.x.x - 11.6.x.x con un valore di build inferiore a 3000 Esempio: 9.5.22. 1760	Versioni del motore di gestione <ul style="list-style-type: none"> 6.x.x.x - 11.7.x.x con un valore di build superiore o pari a 3000 <ul style="list-style-type: none"> Esempio: 11.6.27.3264 2.x.x.x - 5.x.x.x 11.7.x.x o superiore

Nota: la tecnologia Intel® Small Business è lo SKU di gestibilità per Intel® Small Business Advantage

Ampliare l'inventario hardware Microsoft* SCCM per includere i risultati dello strumento console INTEL-SA-00075

Se si sceglie di memorizzare i risultati dello strumento di rilevamento nel Registro di sistema di Windows, è possibile utilizzare l'estensibilità dell'inventario hardware di Microsoft* SCCM per importare i risultati. In questo modo sarà possibile creare raccolte in SCCM da destinare ai computer per la risoluzione dei problemi o gli aggiornamenti del firmware. A tal fine, è necessario eseguire le seguenti operazioni:

1. Aggiungere classi di inventario hardware al file configuration.mof di SCCM
2. Attivare queste nuove classi di inventario hardware nella configurazione del client.
3. Creare un pacchetto software da distribuire ed eseguire lo strumento console INTEL-SA-00075 (Intel-SA-00075-console.exe).
4. Creare una sequenza di attività per eseguire il pacchetto software.

Modifica del file MOF

Nota: se nell'ambiente è presente un server centrale, modificare il file MOF su di esso. In caso contrario, apportare queste modifiche su ogni server primario.

1. Individuare il file configuration.mof. Si trova in genere in \Programmi\Gestione Configurazione Microsoft\inboxex\clifiles.src\hin\
2. Eseguire una copia di backup.
3. Modificare il file configuration.mof, scorrere fino alla fine del file e collocare il cursore sopra questa riga:

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

4. Incollare il contenuto delle modifiche del file MOF nelle pagine 13-14 in questo documento sopra la riga nel passaggio 3.
5. Salvare e chiudere il file.
6. Aprire un prompt dei comandi eseguendolo come amministratore nella directory contenente il file configuration.mof
7. Eseguire mofcomp senza opzioni con destinazione il file configuration.mof modificato.

Inventario hardware - Modifiche

Nota: una volta apportate queste modifiche, ci vorrà un po' di tempo prima che si propaghino ai client e che queste nuove voci appaiano nell'inventario hardware. Il tempo richiesto varierà in base alla configurazione dell'ambiente.

1. Creare un nuovo file denominato INTEL-SA-00075.mof.
2. Incollare il contenuto dell'Importazione Inventario hardware di INTEL-SA-00075 nella pagina 165 nel file appena creato quindi fare clic su Salva.
3. Avviare la console Gestore Configurazione
4. Amministrazione > Impostazioni client > Impostazioni predefinite client
5. Fare doppio clic su Impostazioni predefinite client > Proprietà
6. Selezionare Inventario hardware > Imposta classi
7. Fare clic su Importa.
8. Andare al file di INTEL-SA-00075.mof > Apri.
9. Verificare che siano selezionate l'opzione "Importare entrambe le classi di inventario hardware e le impostazioni di classe di inventario hardware".
10. Fare clic su Importa.
11. OK > OK
12. SCCM registra le modifiche apportate all'inventario hardware nel file dataldr.log

Creare il pacchettoSCCM

1. Creare il file batch come descritto a pag. 15 e inserirlo in una cartella con i file dello strumento console Intel-SA-00075.
2. Avviare la console Gestore Configurazione
3. Libreria software > Pacchetti
4. Fare clic con il pulsante destro del mouse su Pacchetti > Crea pacchetti
5. Nome: Intel-SA-00075
6. Verificare che il pacchetto contenga i file di origine
7. Selezionare la cartella del pacchetto del passaggio 1.

8. Avanti
9. Selezionare Non creare un programma
10. Avanti > Avanti > Chiudi
11. Distribuire il pacchetto nei punti di distribuzione appropriati

Creare una sequenza di attività SCCM

1. Avviare la console Gestore Configurazione
2. Libreria software > Sistemi operativi
3. Fare clic con il pulsante destro del mouse su Sequenze attività > Crea sequenza attività
4. Selezionare Crea una nuova sequenza attività
5. Avanti
6. Inserire il nome Intel-SA-00075
7. Avanti > Avanti > Chiudi
8. Fare clic con il pulsante destro del mouse sulla sequenza di attività Intel-SA-00075, quindi fare clic su Modifica.
9. Aggiungi > Generale > Esegui riga di comando
10. Inserire Intel-SA-00075.bat nel campo Command Line
11. Selezionare la casella Pacchettto, quindi selezionare Sfoglia

12. Seleziona il pacchetto Intel-SA-00075 creato in precedenza > OK
13. Fare clic su OK.

Utilizzo dell'utility System Discovery di Intel® SCS

Che cos'è l'utility System Discovery di Intel® SCS?

L'utility System Discovery di Intel® SCS è un componente della suite Intel® Setup and Configuration Software (Intel® SCS) che fornirà dettagli specifici dell'hardware e del software di un sistema che supporta la tecnologia Intel® Active Management, Intel® Standard Manageability (ISM) o la tecnologia Intel® Small Business. Quando viene eseguita, può salvare i risultati nel Registro di sistema di Microsoft Windows e/o in un file XML. Queste informazioni possono essere utilizzate per individuare i sistemi a cui destinare gli aggiornamenti del firmware o su cui implementare la mitigazione.

Come ottenere l'utility System Discovery di Intel® SCS

Il download del pacchetto Intel® SCS System Discovery Utility è disponibile all'indirizzo <https://downloadcenter.intel.com/download/26691/Intel-SCS-System-Discovery-Utility>.

Determinazione della versione del firmware di gestibilità utilizzando l'utility System Discovery di Intel® SCS

L'output dell'utility System Discovery di Intel® SCS può essere utilizzato per determinare la versione del firmware di un sistema e se il sistema è una SKU di gestibilità. Queste informazioni sono fornite nella sezione `ManageabilityInfo` dei risultati. Per istruzioni su come eseguire il tool, leggere la sezione *Esecuzione dell'utility System Discovery di Intel® SCS* qui di seguito.

Il valore `FWVersion` contiene la versione del firmware attualmente presente sul dispositivo. Il valore `AMTSKU` contiene lo SKU di gestibilità supportato, se presente. Controllare i valori di `FWVersion` e `AMTSKU` per stabilire delle vulnerabilità del sistema, come descritto nella Tabella 6.

Tabella 6. Criteri per determinare se un sistema è vulnerabile agli INTEL-SA-00075 utilizzando la Intel® SCS System Discovery Utility

Nome valore	Vulnerabile	Non vulnerabile
AMTSKU	Intel(R) Full AMT Manageability Intel(R) Standard Manageability Intel(R) Small Business Advantage Output di esempio: <code><ManageabilityInfo> <AMTSKU>Intel(R) Full AMT Manageability</AMTSKU> <AMTversion>11.0.0</AMTversion> <FWVersion>11.0.0.1202</FWVersion></code>	Il valore AMTSKU non è presente nell'output -oppure- I valori AMTSKU a sinistra con una versione del firmware che non è vulnerabile Output di esempio: <code><ManageabilityInfo> <FWVersion>9.0.13.1402</FWVersion></code>
FWVersion	Firmware lo SKU di gestibilità Intel® versioni 6.x.x.x - 11.6.x.x con un valore build inferiore a 3000 Esempio: 9.5.22. <u>1760</u>	Versioni del firmware dello SKU di gestibilità di Intel®: <ul style="list-style-type: none"> 6.x.x.x - 11.7.x.x con un valore di build superiore o pari a 3000 <ul style="list-style-type: none"> Esempio: 11.6.27.<u>3264</u> 2.x.x.x. - 5.x.x.x 11.7.x.x o superiore

Nota: la tecnologia Intel® Small Business è lo SKU di gestibilità per Intel® Small Business Advantage

Esecuzione dell'utility System Discovery di Intel® SCS

Salvare i dati solo nel Registro di sistema

Per eseguire l'utility System Discovery di Intel® SCS e scrivere i dati nel Registro di sistema, da un prompt dei comandi con diritti amministrativi eseguire il seguente comando:

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

Salvare i dati solo in un file XML

Utilizzare il seguente comando per eseguire l'utility System Discovery di Intel® SCS e salvare i dati in un file XML:

```
SCSDiscovery.exe SystemDiscovery <nome file e percorso> /noregistry
```

Il nome del file e il percorso possono essere un percorso locale sul sistema o una condivisione di rete. Se si sceglie di utilizzare una condivisione di rete, accertarsi che l'account che esegue l'utility System Discovery di Intel® SCS abbia le autorizzazioni di scrittura per la condivisione di rete. Se non si specifica un nome di file e un percorso, per il file XML verrà utilizzato il nome di dominio completo del sistema e il file sarà archiviato nella directory che contiene l'utility System Discovery di Intel® SCS.

Salvare i dati nel Registro di sistema e in un file XML

Utilizzare il seguente comando per eseguire l'utility System Discovery di Intel® SCS e salvare i dati nel Registro di sistema e in un file XML:

```
SCSDiscovery.exe SystemDiscovery <nome file e percorso>
```

Come nell'esempio precedente, se non si specifica un nome di file e un percorso, per il file XML verrà utilizzato il nome di dominio completo del sistema e il file sarà archiviato nella directory che contiene l'utility System Discovery di Intel(R) SCS.

Risultati dell'utility System Discovery di Intel® SCS

La quantità di dati restituiti dall'utility System Discovery di Intel® SCS varia se lo stack di driver di gestibilità Intel è caricato nel sistema. Se sono presenti il driver dell'interfaccia del motore di gestione Intel® e Local Management Service (LMS) dell'applicazione Intel® Management and Security, il set di dati disponibile sarà più dettagliato. I risultati riportati di seguito si concentrano solo sui campi di dati di alcune chiavi che sono rilevanti per il problema noto di privilege escalation. Per ulteriori informazioni su altri campi di dati, vedere la documentazione dell'utility System Discovery di Intel® SCS. Alcuni campi potrebbero non essere supportati dal produttore.

Risultati del Registro di sistema

I risultati salvati nel Registro di sistema sono reperibili nella seguente posizione:

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

Valori delle chiavi:

Nome valore	Sottochiave del Registro di sistema	Descrizione del valore
FWVersion	ManageabilityInfo	Versione firmware del motore di gestione Intel®
AMTSKU	ManageabilityInfo	Funzione di gestibilità supportata, se ne è presente una

Risultati del file XML

La versione del firmware del motore di gestione Intel® si trova nel percorso seguente del file XML:

```
<SystemDiscovery>
  <ManageabilityInfo>
    <FWVersion> Numero versione </FWVersion>
```

La funzione di gestibilità supportata del sistema, se è presente, si trova nel percorso seguente del file XML:

```
<SystemDiscovery>
  <ManageabilityInfo>
    <AMTSKU> Nome funzione di gestibilità </AMTSKU>
```

Importazione dei dati di rilevamento del sistema nell'inventario hardware SCCM

Il processo di raccolta dei dati di rilevamento del sistema può essere automatizzato con Intel® SCS Add-on per Microsoft* System Center Configuration Manager (SCCM). Quando è installato, questo componente aggiuntivo estenderà automaticamente l'inventario hardware SCCM includendo i dati di rilevamento del sistema nonché creando sequenze di attività che possono essere usate per eseguire il rilevamento del sistema in relazione a raccolte di sistemi. Le informazioni raccolte tramite questo processo possono essere utilizzate per creare raccolte SCCM con cui inviare gli aggiornamenti del firmware o le mitigazioni ai sistemi interessati.

Il download del pacchetto Intel® SCS Add-On per Microsoft SCCM è disponibile all'indirizzo:

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

Modifiche ai file 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 EHBCEEnabled;
};

[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 =====
```

Importazione Inventario hardware di 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;
};
```

file INTEL-SA-00075.bat batch

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

Esempi di Raccolta query

Computer con Provisioning

```
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 in esecuzione

```
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"
```

LE INFORMAZIONI CONTENUTE IN QUESTO DOCUMENTO SONO FORNITE IN ABBINAMENTO AI PRODOTTI INTEL*. QUESTO DOCUMENTO NON CONCEDE ALCUNA LICENZA, IMPLICITA O ESPlicita, MEDIANTE PRECLUSIONE O ALTRO, PER QUANTO RIGUARDA I DIRITTI DI PROPRIETÀ INTELLETTUALE. AD ECCEZIONE DI QUANTO STABILITO DAI TERMINI E DALLE CONDIZIONI DI VENDITA INTEL PER I PRODOTTI IN QUESTIONE, INTEL NON SI ASSUME ALCUNA RESPONSABILITÀ E DISCONOSCE QUALSIASI GARANZIA ESPRESSA O IMPLICITA RELATIVA ALLA VENDITA E/O ALL'UTILIZZO DI PRODOTTI INTEL, INCLUSA LA RESPONSABILITÀ O L'IDONEITÀ AD UNO SCOPO PARTICOLARE, LA COMMERCIALIZZABILITÀ O LA VIOLAZIONE DI BREVETTI, COPYRIGHT O ALTRI DIRITTI DI PROPRIETÀ INTELLETTUALE. SE NON DIVERSAMENTE CONCORDATO PER ISCRITTO, I PRODOTTI INTEL NON SONO PROGETTATI NÉ DESTINATI AD APPLICAZIONI IN CUI IL GUASTO DEL PRODOTTO INTEL POTREBBE CREARE UNA SITUAZIONE CON POSSIBILI LESIONI PERSONALI O DECESSO.

Le caratteristiche e i vantaggi delle tecnologie Intel dipendono dalla configurazione di sistema e potrebbero richiedere hardware e software abilitati o l'attivazione di servizi. Le prestazioni possono variare a seconda della configurazione del sistema. Nessun sistema informatico può essere totalmente sicuro. Rivolgersi al produttore o al rivenditore del sistema o consultare informazioni più approfondite sul sito intel.it.

Copyright © 2017 Intel Corporation. Tutti i diritti riservati. Intel e il logo Intel sono marchi di Intel Corporation o di società controllate da Intel negli Stati Uniti e/o in altri Paesi.

* Altri marchi e altre denominazioni potrebbero essere rivendicati da terzi.