

INTEL-SA-00075 Leitfaden zu Tools für die Erkennung und Risikominderung von Sicherheitslücken

Intel® Active-Management-Technologie (Intel® AMT), Intel® Standard-Manageability (ISM) und Intel® Small Business Technologie (SBT)

Anleitungen zur Erkennung und Risikominderung von Sicherheitslücken – INTEL-SA-00075

Version 1.1 – 20 Juli 2017

Einführung

Dieses Dokument führt Sie Schritt für Schritt durch die Prozesse zur Erkennung und Risikominderung der in INTEL-SA-00075 beschriebenen Sicherheitslücke. Weitere Informationen dazu finden Sie in der öffentlichen Sicherheitsempfehlung unter <https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr>.

Für Benutzer eines einzelnen PCs, die den Status des PCs erfahren möchten: Für eine lokale Analyse eines Einzel- oder Standalone-Systems bieten wir die INTEL-SA-00075 Benutzeroberflächenanwendung für die Erkennung (Intel-SA-00075-gui.exe).

Zur Bestimmung des Status von mehreren Systemen und/oder zum Anwenden von Risikominderungsmaßnahmen: Wir bieten die INTEL-SA-00075 Tool-Konsolenanwendung für die Erkennung und Risikominderung von Sicherheitslücken an (Intel-SA-00075-console.exe). Dieses Tool kann eine Erkennung durchführen und die Ergebnisse in der lokalen Windows-Registrierung aufzeichnen, und (optional) in einer XML-Datei für nachfolgende Erfassung und Analyse. Die Konsolenanwendung kann auch bei der Implementierung von Risikominderungsmaßnahmen helfen. Unter *Einsatz des INTEL-SA-00075 Tools für die Erkennung und Risikominderung* auf Seite 2 finden Sie weitere Informationen dazu.

Wenn Sie ein Netzwerkadministrator sind, der bereits die Intel® Setup- und Konfigurations-Software (Intel® SCS) nutzt: Die Intel® SCS-Suite umfasst ein alternatives Konsolen-Tool, das Intel® SCS System Discovery Utility (SCS-Systemerkennungsprogramm). Wir empfehlen den Einsatz dieses Tools, wenn Sie bereits mit Intel® SCS-Tools vertraut sind oder genaue Daten über die Intel® AMT erhalten möchten. Siehe *Verwenden des Intel® SCS-Systemerkennungsprogramms* auf Seite 111.

Risikominderung

Die in diesem Dokument beschriebenen Risikominderungsschritte dienen zur Verhinderung nicht autorisierter Aktivierung und dem Einsatz von Intel Manageability-SKUs, Intel® Active-Management-Technologie (Intel® AMT), Intel® Standard-Manageability (ISM) und Intel® Small Business Technologie (SBT), für die die Firmware zur Behebung der Sicherheitslücke nicht angewendet wurde.

IT-Experten können diese Anleitungen als Grundlage für Skripts und Aufgaben in Managementkonsolen für groß angelegte Implementierungen der Risikominderungsschritte verwenden. Die Verfahrensschritte für die Implementierung der Risikominderung sind:

1. Aufheben der Bereitstellung von Intel Manageability SKU-Clients, um das Risiko zu mindern, dass nicht berechnete Netzwerk-Angreifer auf Systemberechtigungen zugreifen
2. Deaktivieren oder Entfernen des Local Manageability Service (LMS), um das Risiko zu mindern, dass nicht berechnete lokale Angreifer auf Systemberechtigungen zugreifen
3. Optional das Konfigurieren von Einschränkungen für die lokale Verwaltbarkeit

Intel empfiehlt dringend, dass der erste Schritt bei allen Risikominderungsschritten die Aufhebung der Bereitstellung der Intel Manageability-SKU ist, um die Netzwerkberechtigung-Eskalations-Sicherheitslücke anzusprechen. Für bereitgestellte Systeme muss die Aufhebung der Bereitstellung vor der Deaktivierung oder dem Entfernen von LMS durchgeführt werden. Je nach Verfügbarkeit der aktualisierten Intel Manageability-SKU-Firmware empfiehlt Intel dringend die Risikominderung der lokalen Berechtigungseskalation durch Entfernen oder Deaktivieren des LMS. Optional können (als zweite Verteidigungsebene vor unbeabsichtigter Neuinstallation oder Neuaktivierung des LMS oder erneutes Aktivieren von LMS) einige der Konfigurationsoptionen, die über das Betriebssystem (BS) ausgeführt werden, zusätzlich über das BS deaktiviert werden; diese zusätzlichen lokalen Manageability-Konfigurationseinschränkungen haben jedoch Beschränkungen bezüglich der Art, wie sie rückgängig gemacht werden können.

Hinweis: AMT 6.0.x unterstützt das Host-Basis-Bereitstellung/Client-Steuerungsmodell nicht, und kann in der Folge nicht über die lokale BS-Benutzeroberfläche über das INTEL-SA-00075 Tool für die Erkennung und Risikominderung aufgehoben werden. Für Plattformen mit Manageability-Firmware 6.0.x.x oder 6.1.x.x wird eine volle Aufhebung der Bereitstellung mit ACUConfig/full der Intel SCS-Suite oder über MEBx der Systeme erforderlich sein.

Wenden Sie sich an den [Intel Kundensupport](#), um Hilfe bei der Implementierung der Risikominderungsschritte in diesem Dokument zu erhalten. Wählen Sie dazu im Bereich „Technologien“ die Intel® Active-Management-Technologie (Intel® AMT).

Einsatz des INTEL-SA-00075 Tools für die Erkennung und Risikominderung

Was ist das INTEL-SA-00075 Tool für die Erkennung und Risikominderung?

Das INTEL-SA-00075 Tool für die Erkennung und Risikominderung kann von lokalen Benutzern oder einem IT-Administrator verwendet werden, um festzustellen, ob ein System für die in der Intel Sicherheitsempfehlung INTEL-SA-00075 dokumentierte Sicherheitslücke anfällig ist. Die Konsolenversion des Tools kann zur Ausführung der Risikominderungsschritte verwendet werden.

Das Tool für die Erkennung und Risikominderung wird in zwei Versionen angeboten.

- Die erste ist ein interaktives GUI-Tool, das bei der Ausführung die Einzelheiten zu Hardware und Software des Geräts ermittelt und eine Risikobewertung liefert. Diese Version wird empfohlen, wenn eine lokale Bewertung des Systems erwünscht ist.
- Die zweite Version ist eine ausführbare Datei für die Konsole, die die Risikobewertung durchführen und die empfohlenen Risikominderungsschritte anwenden kann. Sie kann optional die Erkennungsinformationen in der Windows* Registrierung und/oder in einer XML-Datei speichern. Diese Version empfiehlt sich für IT-Administratoren, die die Erkennungs- und Risikominderungsoperationen über mehrere Computer hinweg durchführen möchten.

So holen Sie sich das INTEL-SA-00075 Tool für die Erkennung und Risikominderung

Das Download-Paket für das INTEL-SA-00075 Tool für die Erkennung und Risikominderung ist verfügbar unter: <https://www.intel.com/content/www/de/de/support/technologies/000024133.html>.

Systemvoraussetzungen

- Microsoft Windows* 7, 8, 8.1 oder 10
- Administratorzugriff auf das lokale Betriebssystem

Installieren des Tools

Interaktive Installation

Führen Sie die Datei INTEL-SA-00075 Detection and Mitigation Tool.msi aus und befolgen Sie die Anleitungen am Bildschirm.

Automatische Installation

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

Dadurch wird das INTEL-SA-00075 Tool für die Erkennung und Risikominderung im Standardverzeichnis installiert:

```
C:\Program Files (x86)\Intel\Intel-SA-00075 Detection and Mitigation Tool\
```

Deinstallieren des Tools

Interaktive Deinstallation

Führen Sie die Datei INTEL-SA-00075 Detection and Mitigation Tool.msi aus und befolgen Sie die Anleitungen am Bildschirm.

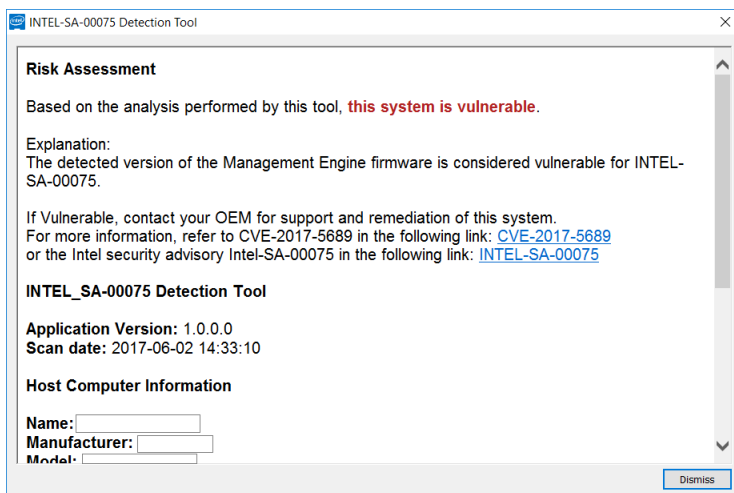
Automatische Deinstallation

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

Ausführen des GUI-Tools

INTEL-SA-00075-GUI.exe ist zum Einsatz auf nur einem System konzipiert. Bei der Ausführung zeigt das Tool die erkannten Informationen am Bildschirm an.

Abbildung 1. Beispiel der Ausgabe von INTEL-SA-00075-GUI am Bildschirm



Ausführen des Konsolen-Tools

Führen Sie `INTEL-SA-00075-console.exe` von einer Eingabeaufforderung mit Administratorrechten aus.

Einsatz:

```
Intel-SA-00075-console.exe [[Befehl] | [Option...]]
```

Es kann jeweils nur ein Befehl ausgeführt werden. Wenn kein Befehl angegeben ist, wird der Discover-Befehl zur Erkennung ausgeführt.

Tabelle 1. INTEL-SA-00075 Konsole-Befehlszeilenparameter

Befehlszeilenbefehl	Funktion
-Discover	Ausgabe der Ergebnisse an die Konsole und Schreiben der Daten in die Registrierung.
-Unprovision [password], -u [password]	Entfernen aller Intel AMT-Einstellungen und Deaktivieren der Funktionen von Intel AMT; ein Admin-Benutzerkennwort kann für das Intel AMT-Gerät verwendet werden und ist möglicherweise erforderlich. HINWEIS: Das Aufrufen dieses Befehls ohne Kennwort funktioniert nur mit Firmware-Versionen, die von INTEL-SA-00075 (6.1.x.x–11.6.x.x mit einer Build-Nummer unter 3000) betroffen sind. Wenn Sie die Firmware-Versionen 6.1.x.x–11.6.x.x mit einer Build-Nummer höher als 3000 verwenden, funktioniert die Aufhebung der Bereitstellung nur, wenn Sie ein Kennwort eingeben.
-DisableClientControlMode, -DisableCCM	Dauerhafte Deaktivierung der Client-Steuerung-Modusoption im Intel AMT-Gerät. Nach der Ausführung dieses Befehls kann das Gerät nicht in den Client-Steuerungsmodus gesetzt werden. HINWEIS: Es gibt keinen CLI-Befehl, um diesen Vorgang rückgängig zu machen. WARNUNG: Nicht alle Plattformen können CCM nach der Deaktivierung erneut aktivieren.
-DisableLMS	Deaktiviert den LMS-Service.

Befehlszeilenoption	Funktion
-n, -noregistry	Verhindert das Schreiben der Ergebnisse in die Registrierung
-c, -noconsole	Verhindert, dass die Ergebnisse auf der Konsole angezeigt werden
-d, -delay <seconds>	Verzögerung in Sekunden vor Beginn der Ausführung. Wenn kein Wert angegeben wird, hat das Tool keine Verzögerung.
-f, -writefile	Spezifiziert das Schreiben der Ergebnisse in eine Datei. Der Dateiname hat das folgende Format: <Computername>.xml
-p <filepath>, -filepath <filepath>	Der Speicherpfad für die Ausgabedatei. Wenn kein Pfad angegeben ist, wird die Datei in das Verzeichnis geschrieben, von dem aus das Tool ausgeführt wird.
-h, -help, -?	Zeigt diese Befehlszeilenparameter und deren Funktionen an.

-Discover

Der Discover-Befehl gibt die erkannten Informationen an die Konsole aus. Standardmäßig werden die Erkennungsinformationen auch in die Registrierung geschrieben. Wenn kein Befehl an das Konsolen-Tool ausgegeben wird, wird der Discover-Befehl ausgeführt.

-Unprovision

Entfernt alle Intel AMT-Einstellungen und deaktiviert die AMT-Funktionen; ein optionales Admin-Benutzerkennwort kann für das Intel AMT-Gerät verwendet werden.

Wenn entsprechend konfiguriert, hören Intel® AMT und ISM automatisch den Verwaltungsverkehr über Ihr Computernetzwerk ab. Für Systeme, die für das bekannte Berechtigungs eskalations-Problem anfällig sind, sollte die Bereitstellung mit dem Unprovision-Befehl aufgehoben werden, um nicht autorisierten Zugriff auf Verwaltungsfunktionen zu verhindern.

Das Aufrufen dieses Befehls ohne Kennwort funktioniert nur mit Firmware-Versionen, die von INTEL-SA-00075 (6.1.x.x–11.6.x.x mit einer Build-Nummer unter 3000) betroffen sind. Wenn Sie die Firmware-Versionen 6.1.x.x–11.6.x.x mit einer Build-Nummer höher als 3000 verwenden, funktioniert die Aufhebung der Bereitstellung nur, wenn Sie ein Kennwort eingeben.

-DisableClientControlMode

Die -DisableClientControlMode Konfigurationseinschränkung ist ein optionaler Schritt für Kunden, die eine zweite Ebene zum Schutz

vor Risikominderung-Umkehrung durch einen nicht berechtigten Angreifer, der BS-Administratorberechtigungen erlangt, erfordern. Die Umkehrung dieser Optionen ist schwierig, wird unter Umständen nicht vom Computerhersteller unterstützt, und erfordert möglicherweise physischen Zugriff auf das System. Wenn Sie diese zusätzliche Konfigurationseinschränkung durchführen möchten, muss dies vor der Deaktivierung des LMS-Service erfolgen.

Schritte zur Neuaktivierung von CCM

Wenn dies vom Hersteller unterstützt wird, können Sie die Intel Manageability-SKUs möglicherweise vom BIOS aus zurücksetzen, was die Neuaktivierung von CCM zur Folge hätte. Fragen Sie bei Ihrem Hersteller nach, ob diese Funktion unterstützt wird und welche Schritte dazu zu befolgen sind.

Hinweis: Ihr Hersteller kann Ihnen möglicherweise Tools bereitstellen, mit denen Sie die BIOS-Einstellungen über das Betriebssystem konfigurieren können. Mit diesen Tools (falls verfügbar) können Sie unter Umständen die Intel Manageability-SKUS im BIOS zurücksetzen, ohne physisch auf den Computer zugreifen zu müssen. Fragen Sie bei Ihrem Hersteller nach, ob ein Tool mit dieser Funktionalität angeboten wird.

-DisableLMS

Der Befehl DisableLMS deaktiviert den LMS-Service als Risikominderungsschritt.

Was ist LMS?

Intel® Management and Security Application Local Management Service (LMS) ist ein Service, der es lokalen Anwendungen, die auf Geräten, die auf Intel® AMT, Intel® SBA oder Intel® Standard Manageability ausgeführt werden, ermöglicht, die geläufige SOAP- und WS-Management-Funktionen zu nutzen. Er hört die Intel® Manageability Engine (ME) Ports (16992, 16993, 16994, 16995, 623 und 664) ab und leitet den Datenverkehr über den Intel® MEI-Treiber an die Firmware weiter.

Weitere Überlegungen

Jeder Benutzer mit BS-Administratorrechten kann den LMS neu installieren, wenn er entfernt wird, oder den Dienst erneut aktivieren, wenn er deaktiviert ist. Daher ist es wichtig, umsichtig vorzugehen, um eine versehentliche Neuinstallation oder Neuaktivierung von LMS zu vermeiden, während die Sicherheitslücke auf dem System vorhanden ist. Beispielsweise könnte der LMS neu installiert werden, wenn Sie das Installationsprogramm für die Intel Manageability-Software zukünftig ausführen.

Abbildung 2. Beispiel für INTEL-SA-00075-Konsolen-Ausgabe

```
INTEL-SA-00075 Erkennungstool
Anwendungsversion: <Anwendungsversion>
Scan-Datum: <Datum und Uhrzeit>

*** Host-Computer-Informationen***
Computer-Name: <Computername>
Hersteller: <Computerhersteller>
Modell: <Computermodell>
Prozessor: <Prozessormodell>
Windows-Version: <Windows* Version>

*** ME-Informationen ***
Version: <Intel ME Firmware-Version>
SKU: <Manageability-Funktion, falls vorhanden>
Zustand: <ME-Bereitstellungszustand>
Installierter Treiber: <True/False>
Steuerungsmodus: <Keiner/ACM/CCM>
Falls CCM deaktiviert: <True/False/Nicht bekannt>
EHBC aktiviert <True/False>
LMS-Zustand: <Läuft/Gestoppt/Nicht vorhanden>
LMS-Startup-Typ: <Boot/System/Auto/Manuell/Deaktiviert/Nicht vorhanden>
MicroLMS-Zustand: <Läuft/Gestoppt/Nicht vorhanden>
MicroLMS-Startup-Typ: <Boot/System/Auto/Manuell/Deaktiviert/Nicht vorhanden>
Ist SPS: <True/False>
```

*** Risikobewertung ***

Basierend auf der von diesem Tool ausgeführten Analyse,

< dieses System ist anfällig /

dieses System ist nicht anfällig /

dieses System ist nicht anfällig; nicht-Intel SKU /

dieses System ist nicht anfällig; die ME-FW-Version ist nicht betroffen /

dieses System ist nicht anfällig; die ME-SKU ist nicht betroffen /

dieses System ist nicht anfällig; das SMBIOS gibt an, dass es sich um ein Kunden-SKU handelt /

dieses System ist nicht anfällig; das System wird auf SPS-FW ausgeführt (Server-Plattform-Services-Firmware) /

die Firmware dieses Systems wurde aktualisiert und das System befindet sich nicht im bereitgestellten Zustand /

die Firmware dieses Systems wurde aktualisiert und das System befindet sich im bereitgestellten Zustand /

Bei OEM nachfragen /

das Risiko dieses Systems ist nicht bekannt>

Falls anfällig, wenden Sie sich an Ihren OEM für Support und Problembeseitigung des Systems.

*** Weitere Informationen ***

Siehe CVE-2017-5689 unter:

<https://nvd.nist.gov/vuln/detail/CVE-2017-5689>

oder die Intel Sicherheitsempfehlung Intel-SA-00075 unter:

<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr>

Die zur Bestimmung einer Risikobewertung verwendete Logik wird in Tabelle 2 beschrieben.

Tabelle 2. Bedeutung der Risikobewertung in der Ausgabe

Nachricht	Bedeutung
Anfällig	Die erkannte Version der Management-Engine-Firmware gilt für INTEL-SA-00075 als anfällig.
Nicht anfällig	Das System erfüllt die „Nicht anfällig“-Kriterien wie beschrieben unter <i>Identifizieren betroffener Systeme mit dem INTEL-SA-00075 Erkennungstool</i> auf Seite 8.
Die Firmware dieses Systems wurde aktualisiert und das System befindet sich nicht im bereitgestellten Zustand	Die erkannte Firmware auf diesem System verfügt über die Fehlerbehebung INTEL-SA-00075. Stellen Sie vor der erneuten Bereitstellung sicher, dass die INTEL-SA-00075 Tools zur Durchführung einer vollständigen Aufhebung der Bereitstellung des Systems verwendet wurden. Dadurch werden alle nicht autorisierten Konfigurationseinstellungen entfernt.
Die Firmware dieses Systems wurde aktualisiert und System befindet sich im bereitgestellten Zustand	Die erkannte Firmware auf diesem System verfügt über die Fehlerbehebung INTEL-SA-00075. Wenn das System vor der Aktualisierung der Firmware bereitgestellt wurde, werden durch eine vollständige Aufhebung der Bereitstellung und eine erneute Bereitstellung des Systems alle nicht autorisierten Konfigurationseinstellungen entfernt.
Bei OEM nachfragen	Die erkannten Informationen im SMBIOS vom OEM zeigen eine Manageability-SKU, aber das Tool hat keine Antwort erhalten, als detaillierte Daten von Ihrem Computer angefordert wurden. Dies kann durch einen fehlenden Management-Engine-Schnittstellentreiber verursacht werden. Wenden Sie sich an Ihren OEM, um herauszufinden, ob Ihr Computermodell betroffen ist.

Nachricht	Bedeutung
Nicht bekannt	<p>Das Tool hat keine gültige Antwort erhalten, als Hardwareinventur-Daten von Ihrem Computer angefordert wurden. Wenden Sie sich an den Systemhersteller, um Hilfe bei der Identifizierung der Sicherheitslücke des Systems zu erhalten.</p> <p>Diese Meldung kann auf einer Serverplattform ohne installierten PMX-Treiber angezeigt werden. Dieser Treiber ist unter Umständen nicht auf allen Versionen des Windows-Betriebssystems verfügbar. Wenn der Treiber nicht vorhanden ist, ist die empfohlene Fehlerumgehung das Ausführen der spsInfo- oder spsManuf-Anwendung, die mit der SPS-Firmware-Version bereitgestellt werden. Beide Anwendungen installieren den PMX-Treiber.</p>

Ergebnisse

Hinweis: Die Menge der vom INTEL-SA-00075 Discover-Befehl zurückgegebenen Daten hängt davon ab, ob der Intel Manageability-Treiber-Stack auf dem System geladen ist. Wenn der Treiber für die Intel® Management Engine Interface (MEI) und den Intel® Management and Security Application Local Management Service (LMS) vorhanden sind, wird ein ausführlicher Datensatz verfügbar sein. Einige Felder werden u. U. nicht vom Hersteller unterstützt.

Registrierungs-Speicherort

Die Werte in der Ergebnistabelle finden Sie im folgenden Registrierungsschlüssel:

- 32-Bit-Betriebssysteme: HKLM\SOFTWARE\
Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool
- 64-Bit-Betriebssysteme: HKLM\SOFTWARE\WOW6432Node\
Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool

XML

Wenn Sie sich entscheiden, die Ergebnisse in eine XML-Datei zu schreiben, wird diese Datei im Verzeichnis gespeichert, aus dem INTEL-SA-00075-console.exe ausgeführt wird, oder in dem in den Befehlszeilenoptionen angegebenen Pfad. Informationen wie die Hardwareinventur, das BS und das Vorhandensein von LMS sind eingeschlossen. Wenn AMT vorhanden ist, ist die Liste der gefundenen standardmäßigen und angepassten Zertifikat-Hashes eingeschlossen. Diese Liste kann verwendet werden, um erwartet Hashes mit den tatsächlich in AMT gespeicherten zu vergleichen.

Konsolen-Rückgabecodes

Tabelle 3. INTEL-SA-00075 Konsolen-Rückgabecodes

Nummer	Bedeutung
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

Nummer	Bedeutung
506	DISCOVERY_UNKNOWN_CPU

Tabelle 4. INTEL-SA-00075 Konsolenausgabewerte

Wert	Standort	Beschreibung
Application Version (Anwendungsversion)		Die Version des verwendeten Scan-Tools
Scan Date (Scan-Datum)		Das Datum und die Uhrzeit, zu denen der Scan stattfand
Computer Name (Computername)		Der Name des gescannten Computers
Computer Manufacturer (Computerhersteller)	Hardwareinventur	Der Hersteller des Computers
Computer Model (Computermodell)		Das Modell des Computers
Processor (Prozessor)		Das Prozessormodell des Computers
ME Version (ME-Version)	ME-Firmware-Informationen	Ein String-Wert mit der vollständigen ME-Firmware-Versionsnummer im folgenden Format: Major.Minor.Hotfix.Build
ME SKU		Wenn vorhanden, die Manageability-Funktion auf dem System
ME Provisioning State (ME-Bereitstellungszustand)		Der ME-Konfigurationszustand Keiner erkannt Nicht bereitgestellt Bereitstellung in Bearbeitung Bereitgestellt
ME Driver Installed (ME-Treiber installiert)		True/False-Wert, wenn der MEI-Treiber auf dem Computer vorhanden ist
EHBC Enabled (EHBC aktiviert)		True/False-Wert, wenn das System die Bereitstellungsmethode mit der auf dem integrierten Host basierten Konfiguration unterstützt
LMS state (LMS-Zustand)		Informationen dazu, ob der LMS-Service ausgeführt wird, nicht ausgeführt wird oder nicht vorhanden ist
LMS startup type (LMS-Startup-Typ)		Informationen dazu, ob der LMS-Startup-Typ Nicht vorhanden, Boot, System, Auto, Manuell oder Deaktiviert ist
MicroLMS state (MicroLMS-Zustand)		Informationen dazu, ob der MicroLMS-Service ausgeführt wird, nicht ausgeführt wird oder nicht vorhanden ist
MicroLMS startup type (MicroLMS-Startup-Typ)		Informationen dazu, ob der MicroLMS-Startup-Typ Nicht vorhanden, Boot, System, Auto, Manuell oder Deaktiviert ist
Control Mode (Steuerungsmodus)		Der ME-Konfigurationsmodus Keiner, ACM oder CCM
Is CCM Disabled (Ist CCM deaktiviert)		True/False/Nicht Bekannt-Status für den Client-Steuerungsmodus deaktiviert
Ist SPS		Ist die Plattform ein nicht anfälliges Server-Plattform-Services (SPS) System?
*** Risikobewertung ***	Risikobewertung	Siehe <i>Tabelle 2. Bedeutung der Risikobewertung in der Ausgabe</i>

Identifizieren betroffener Systeme mit dem INTEL-SA-00075 Erkennungstool

Betroffene Systeme werden definiert als Systeme, die eine betroffene Intel® Management Engine (ME) Firmwareversion sowie eine der drei Manageability-Feature Sets-enthalten, wie definiert in Tabelle 5.

Hinweis: Server-Plattform-Services (SPS) Plattformen sind nicht anfällig für INTEL-SA-00075. SPS-Plattformen haben Firmware, auf denen die Manageability Engine (ME) (Teil von PCH) auf Server-Plattformen ausgeführt wird. Diese Firmware ist anders als die Intel Manageability-Firmware (die auch auf ME ausgeführt wird) auf PC/Workstation-Plattformen.

Tabelle 5. Kriterien zur Bestimmung, ob ein System anfällig für INTEL-SA-00075 mit dem INTEL-SA-00075 Erkennungstool ist

Name des Werts	Anfällig	Nicht anfällig
ME SKU	Intel® Volle AMT-Manageability Intel® Standard-Manageability Intel® Small Business Advantage (SBA)	ME SKU-Werte nicht in der Liste der anfälligen Systeme auf der linken Seite aufgeführt -oder- MIR SKU-Werte links mit einer Firmware-Version,

ME-Version	ME-Versionen 6.x.x.x – 11.7.x.x mit einem Build unter 3000 Beispiel: 9.5.22. <u>1760</u>	die nicht anfällig ist MIR-Versionen: <ul style="list-style-type: none"> • 6.x.x.x – 11.7.x.x mit einem Build größer oder gleich 3000 <ul style="list-style-type: none"> ◦ Beispiel: 11.6.27.<u>3264</u> • 2.x.x.x. – 5.x.x.x • 11.7.x.x oder höher
------------	---	---

Hinweis: Intel® Small Business Technologie (SBT) ist die Manageability-SKU für Intel® Small Business Advantage (SBA).

Erweiterung der Microsoft* SCCM-Hardwareinventur, um die INTEL-SA-00075 Konsolen-Tool-Ergebnisse aufzunehmen

Wenn Sie wählen, die Ergebnisse des Intel-SA-00075 Konsolen-Tools in der Windows Registrierung zu speichern, können Sie die Microsoft* SCCM-Hardwareinventur-Erweiterung nutzen, um die Ergebnisse zu importieren. Dadurch können Sie Sammlungen in SCCM aufbauen, um diese auf Computern für Fehlerbehebungen und Firmware-Updates anzuwenden. Dazu müssen Sie Folgendes tun:

1. Fügen Sie Hardwareinventur-Klassen zur SCCM-Datei configuration.mof hinzu.
2. Aktivieren Sie diese neuen Hardwareinventur-Klassen in Ihrer Client-Konfiguration.
3. Erstellen Sie ein Softwarepaket zur Bereitstellung und Ausführung des INTEL-SA-00075 Konsolen-Tools (Intel-SA-00075-console.exe).
4. Erstellen Sie eine Aufgabensequenz zur Ausführung des Softwarepakets.

Ändern der MOF-Datei

Hinweis: Wenn Sie einen zentralen Server in Ihrer Umgebung haben, nehmen Sie die MOF-Dateiänderung darauf vor. Nehmen Sie diese Änderungen andernfalls auf allen Ihren primären Servern vor.

1. Suchen Sie nach der Datei configuration.mof. Sie befindet sich in der Regel unter \Programme\Microsoft Configuration Manager\inbox\clfiles.src\hin\
2. Erstellen Sie eine Sicherungskopie.
3. Bearbeiten Sie die Datei configuration.mof, indem Sie am Ende der Datei den Cursor über dieser Zeile setzen:

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

4. Fügen Sie den Inhalt der MOF-Dateiänderungen auf Seite 13-14 in diesem Dokument über der Zeile von Schritt 3 hinzu.
5. Speichern Sie und schließen Sie die Datei.
6. Starten Sie eine Eingabeaufforderung als Administrator im Verzeichnis mit configuration.mof.
7. Führen Sie mofcomp ohne Switches aus, und mit Abzielung auf die abgeänderte Datei configuration.mof.

Änderungen an der Hardwareinventur

Hinweis: Nachdem diese Änderungen vorgenommen wurden, braucht es etwas Zeit für die Verbreitung an Ihre Clients, bevor diese neuen Elemente in der Hardwareinventur angezeigt werden. Die benötigte Zeit dazu variiert je nach der Konfiguration Ihrer Umgebung.

1. Erstellen Sie eine neue Datei mit dem Namen INTEL-SA-00075.mof.
2. Fügen Sie den Inhalt von Importieren der INTEL-SA-00075 Hardwareinventur auf Seite 155 in die neu erstellte Datei ein und

speichern Sie sie.

3. Starten Sie die Konfigurationsmanager-Konsole.
4. Verwaltung > Clienteneinstellungen > Standard-Clienteneinstellungen.
5. Klicken Sie mit der rechten Maustaste auf „Standard-Clienteneinstellungen“ > „Eigenschaften“.
6. Wählen Sie die „Hardwareinventur“ > „Klassen festlegen“.
7. Klicken Sie auf „Importieren“.
8. Navigieren Sie zur Datei INTEL-SA-00075.mof > „Öffnen“.
9. Stellen Sie sicher, dass die Option „Hardwareinventurklassen und Einstellungen für Hardwareinventurklassen importieren“ ausgewählt ist.
10. Klicken Sie auf „Importieren“.
11. OK > OK.
12. SCCM zeichnet die Änderungen an der Hardwareinventur in der Datei dataldr.log auf.

Erstellen des SCCM-Pakets

1. Erstellen Sie die Batch-Datei von Seite 15 und legen Sie sie im Ordner mit der INTEL-SA-00075 Konsolen-Tool-Datei ab.
2. Starten Sie die Konfigurationsmanager-Konsole.
3. Software-Bibliothek > Pakete.
4. Klicken Sie mit der rechten Maustaste auf „Pakete > Paket erstellen“.
5. Name: Intel-SA-00075.
6. Überprüfen Sie, dass dieses Paket die Quelldateien enthält.
7. Wechseln Sie zum Paketordner aus Schritt 1.
8. Weiter.
9. Wählen Sie „Kein Programm erstellen“.
10. Weiter > Weiter > Schließen.
11. Verteilen Sie das Paket an die entsprechenden Verteilungspunkte.

Erstellen einer SCCM Aufgabensequenz

1. Starten Sie die Konfigurationsmanager-Konsole.
2. Software-Bibliothek > Betriebssysteme.
3. Klicken Sie mit der rechten Maustaste auf „Tasksequenzen“ > „Tasksequenz erstellen“.
4. Wählen Sie „Neue benutzerdefinierte Tasksequenz erstellen“ aus.
5. Weiter.
6. Geben Sie den Namen von Intel-SA-00075 ein.
7. Weiter > Weiter > Schließen.
8. Klicken Sie mit der rechten Maustaste auf die Intel-SA-00075 Tasksequenz und klicken Sie auf „Bearbeiten“.
9. Hinzufügen > Allgemein > Befehlszeile ausführen.
10. Geben Sie Intel-SA-00075.bat im Befehlszeilenfeld ein.
11. Überprüfen Sie das Paketfeld und klicken Sie auf „Durchsuchen“.

12. Wählen Sie das zuvor erstellte Intel-SA-00075-Paket > OK.

13. Klicken Sie auf OK.

Verwenden des Intel® SCS-Systemerkennungsprogramms

Was ist das Intel® SCS-Systemerkennungsprogramm?

Das Intel® SCS-Systemerkennungsprogramm ist ein Bestandteil der Intel® Setup- und Konfigurations-Software (Intel® SCS), über die Einzelheiten der Hardware und Software auf einem System bereitgestellt werden, welche die Intel® Active-Management-Technologie (Intel® AMT), Intel® Standard-Manageability (ISM) oder die Intel® Small Business Technologie (Intel® SBT) unterstützen. Bei der Ausführung können die Ergebnisse in die Microsoft Windows Registrierung oder eine XML-Datei gespeichert werden. Diese Informationen können verwendet werden, um Systeme für Firmware-Updates oder zur Implementierung von Risikominderungsmaßnahmen zu finden.

So holen Sie sich das Intel® SCS-Systemerkennungsprogramm

Das Download-Paket für das Intel® SCS-Systemerkennungsprogramm ist verfügbar unter <https://downloadcenter.intel.com/download/26691/Intel-SCS-System-Discovery-Utility>.

Ermitteln der Manageability-Firmware-Version mithilfe des Intel® SCS-Systemerkennungsprogramms

Die Ausgabe des Intel® SCS-Systemerkennungsprogramms kann verwendet werden, um die Firmware-Version eines Systems zu bestimmen und ob das System eine Manageability-SKU ist. Diese Informationen werden im Abschnitt `ManageabilityInfo` der Ausgabe bereitgestellt. Anleitungen zur Ausführung des Tools finden Sie im Abschnitt *Ausführen des Intel® SCS-Systemerkennungsprogramms* auf Seite 12.

Der Wert `FWVersion` enthält die Version der aktuellen Firmware auf dem Gerät. Der Wert `AMTSSKU` enthält die unterstützte Manageability-SKU, sofern vorhanden. Überprüfen Sie die Werte von `FWVersion` und `AMTSSKU`, um die Anfälligkeit Ihres Systems zu bestimmen, wie beschrieben in Tabelle 6.

Tabelle 6. Kriterien zur Bestimmung, ob ein System anfällig für INTEL-SA-00075 ist, unter Einsatz des Intel® SCS-Systemerkennungsprogramms

Name des Werts	Anfällig	Nicht anfällig
AMTSKU	Intel(R) Volle AMT-Manageability Intel(R) Standard-Manageability Intel(R) Small Business Advantage (SBA) Beispielausgabe: <code><ManageabilityInfo> <AMTSKU>Intel(R) Full AMT Manageability</AMTSKU> <AMTversion>11.0.0</AMTversion> <FWVersion>11.0.0.1202</FWVersion></code>	AMTSKU-Wert nicht in der Ausgabe vorhanden -oder- AMTSKU-Werte links mit einer Firmware-Version, die nicht anfällig ist Beispielausgabe: <code><ManageabilityInfo> <FWVersion>9.0.13.1402</FWVersion></code>
FWVersion	Intel® Manageability-SKU-Firmware-Versionen 6.x.x.x – 11.7.x.x mit einem Build unter 3000 Beispiel: 9.5.22. 1760	Intel® Manageability-SKU-Firmware-Versionen: <ul style="list-style-type: none"> 6.x.x.x – 11.7.x.x mit einem Build größer oder gleich 3000 <ul style="list-style-type: none"> Beispiel: 11.6.27.3264 2.x.x.x. – 5.x.x.x 11.7.x.x oder höher

Hinweis: Intel® Small Business Technologie (SBT) ist die Manageability-SKU für Intel® Small Business Advantage (SBA).

Ausführen des Intel® SCS-Systemerkennungsprogramms

Speichern von Daten nur in der Registrierung

Führen Sie den folgenden Befehl von einer Eingabeaufforderung mit Administratorrechten aus, um das Intel® SCS-Systemerkennungsprogramm auszuführen und Daten in die Registrierung zu schreiben:

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

Speichern von Daten nur in eine XML-Datei

Verwenden Sie den folgenden Befehl, um das Intel® SCS-Systemerkennungsprogramm auszuführen und Daten in eine XML-Datei zu schreiben:

```
SCSDiscovery.exe SystemDiscovery <Dateiname und Pfad> /noregistry
```

Der Dateiname und -pfad können sich in einem lokalen Verzeichnis oder auf einer Netzwerkfreigabe befinden. Wenn Sie eine Netzwerkfreigabe verwenden, stellen Sie sicher, dass das Konto, über das das Intel® SCS-Systemerkennungsprogramm ausgeführt wird, über Schreibberechtigung für diese Netzwerkfreigabe verfügt. Wenn Sie keinen Namen und Pfad angeben, wird die FQDN des Systems als XML-Dateiname verwendet werden und die Datei wird im Verzeichnis gespeichert, welches das Intel® SCS-Systemerkennungsprogramm enthält.

Speichern von Daten in der Registrierung und in eine XML-Datei

Verwenden Sie den folgenden Befehl, um das Intel® SCS-Systemerkennungsprogramm auszuführen und Daten in die Registrierung und eine XML-Datei zu schreiben

```
SCSDiscovery.exe SystemDiscovery <Dateiname und Pfad>
```

Wenn Sie wie im obigen Beispiel keinen Namen und Pfad angeben, wird die FQDN des Systems als XML-Dateiname verwendet werden und die Datei wird im Verzeichnis gespeichert, welches das Intel(R) SCS-Systemerkennungsprogramm enthält.

Ergebnisse des Intel® SCS-Systemerkennungsprogramms

Die Menge der vom Intel® SCS-Systemerkennungsprogramm zurückgegebenen Daten hängt davon ab, ob der Intel Manageability-Treiber-Stack auf dem System geladen ist. Wenn der Treiber für die Intel® Management Engine Interface (MEI) und den Intel® Management and Security Application Local Management Service (LMS) vorhanden sind, wird ein ausführlicher Datensatz verfügbar sein. Die unten beschriebenen Ergebnisse konzentrieren sich auf ein paar wichtige Datenfelder, die für das Berechtigungs eskalations-Problem relevant sind. Weitere Informationen zu den anderen Datenfeldern finden Sie in der Dokumentation zum Intel® SCS-Systemerkennungsprogramm. Einige Felder werden u. U. nicht vom Hersteller unterstützt.

Registrierungsergebnisse

Die in der Registrierung gespeicherten Ergebnisse finden Sie an folgendem Speicherort:

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

Wichtige Werte:

Name des Werts	Sub-Schlüssel der Registrierung	Beschreibung des Werts
FWVersion	ManageabilityInfo	Intel® Management-Engine-Firmware-Version
AMTSKU	ManageabilityInfo	Unterstützte Manageability-Funktion, falls vorhanden

Ergebnisse der XML-Datei

Die Intel® Management-Engine-Firmwareversion befindet sich unter folgendem Pfad in der XML:

```
<SystemDiscovery>
  <ManageabilityInfo>
    <FWVersion> Versionsnummer </FWVersion>
```

Die unterstützte Manageability-Funktion des Systems, falls vorhanden, befindet sich unter folgendem Pfad in der XML:

```
<SystemDiscovery>
  <ManageabilityInfo>
    <AMTSKU> Manageability-Funktionsname </AMTSKU>
```

Importieren von Systemerkennungsdaten in die SCCM-Hardwareinventur

Die Erfassung von Systemerkennungsdaten kann mit dem Intel® SCS Add-on für den Microsoft* System Center Configuration Manager (SCCM) automatisiert werden. Bei der Installation erweitert dieses Add-on automatisch die Hardwareinventur, um die Erkennungsdaten des Systems aufzunehmen und Tasksequenzen zu erstellen, die verwendet werden können, um die Systemerkennung im Vergleich zu einer Sammlung von Systemen auszuführen. Die in diesem Verfahren erfassten Daten können dann verwendet werden, um SCCM-Sammlungen zu verwenden, um dann Firmware-Updates oder Risikominderungsmaßnahmen per Push-Verfahren an die betroffenen Systeme zu leiten.

Das Download-Paket für das Intel® SCS Add-on für Microsoft SCCM ist verfügbar unter

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

Änderungen an der MOF-Datei

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

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

Importieren der INTEL-SA-00075 Hardwareinventur

```
#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;
};
```

INTEL-SA-00075.bat Batch-Datei

```
@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%
```

Beispiele für eine Sammlungsabfrage

Bereitgestellte Computer

```
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 wird ausgeführt

```
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"
```

SOLCHER PRODUKTE VORGESEHEN. SOFERN NICHT SCHRIFTLICH VON INTEL ANDERWEITIG FESTGELEGT, SIND DIE INTEL PRODUKTE NICHT FÜR IRGENDWELCHE ANWENDUNGEN KONZIPIERT, BEI DENEN EIN FEHLVERSAGEN DES INTEL PRODUKTS EINE SITUATION HERBEIFÜHREN KÖNNTE, DIE ZU PERSONENVERLETZUNGEN ODER TOD FÜHREN KANN.

Die Funktionsmerkmale und Vorteile von Intel Technologien hängen von der Systemkonfiguration ab und können kompatible Hardware, Software oder die Aktivierung von Services erfordern. Die Leistungsmerkmale variieren je nach Systemkonfiguration. Kein Computersystem bietet absolute Sicherheit. Informieren Sie sich beim Systemhersteller oder Einzelhändler oder unter intel.com.

Copyright © 2017 Intel Corporation. Alle Rechte vorbehalten. Intel und das Intel Logo sind Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

* Alle anderen Marken oder Produktnamen sind Eigentum der jeweiligen Inhaber.