

INTEL-SA-00075 검출 및 완화 도구

안내서

Intel® Active Management Technology(Intel® AMT), Intel® Standard Manageability(ISM) 및 Intel® Small Business Technology(SBT)

INTEL-SA-00075 검출 및 완화 지침

개정 1.1 – 2017 년 7 월 20 일

소개

이 문서에서는 INTEL-SA-00075에 설명된 보안 취약성 검출 및 완화를 위한 여러 과정을 안내합니다. 자세한 내용은 <https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr>의 공개 보안 자문 정보를 읽어보십시오.

단일 PC 사용자이며 PC의 상태 확인을 원하는 경우: 단일 또는 독립형 시스템의 로컬 분석을 위해 INTEL-SA-00075 검색 GUI 애플리케이션(Intel-SA-00075-gui.exe)을 활용하십시오.

여러 기계를 대상으로 한 상태 확인 및/또는 완화 적용을 원하는 경우: INTEL-SA-00075 검출 및 완화 도구 콘솔 애플리케이션(Intel-SA-00075-console.exe)을 활용하십시오. 이 도구는 검색을 수행하여 후속 수집과 분석을 위해 검색 결과를 로컬 Windows 레지스트리와 (선택적으로) XML 파일에 쓸 수 있습니다. 또한 콘솔 애플리케이션이 완화 구현을 지원할 수 있습니다. 자세한 내용은 2페이지의 *INTEL-SA-00075 검출 및 완화 도구 사용*을 참조하십시오.

인텔® 설정 및 구성 소프트웨어(인텔® SCS)를 이미 사용하고 있는 네트워크 관리자인 경우: 인텔® SCS 제품군은 대체 콘솔 도구인 인텔® SCS 시스템 검색 유틸리티를 포함합니다. 인텔® SCS 도구에 이미 익숙하거나 Intel® AMT 관련 상세 데이터를 얻고 싶은 경우 이 도구를 사용할 것을 권장합니다. 131페이지의 *인텔® SCS 시스템 검색 유틸리티 사용*을 참조하십시오.

완화

이 문서에 설명된 완화 단계는 취약성을 해결하는 펌웨어 업데이트를 적용하지 않은 인텔 관리 SKU, Intel® Active Management Technology(Intel® AMT), Intel® Standard Manageability(ISM) 및 Intel® Small Business Technology(SBT)의 승인되지 않은 활성화 및 사용 방식을 목적으로 합니다.

IT 전문가는 이러한 지침을 완화 단계의 대용량 배포를 위한 관리 콘솔 내 스크립트 또는 작업의 기반으로 사용할 수 있습니다. 완화 구현을 위한 단계는 다음과 같습니다.

1. 권한 없는 네트워크 공격자의 시스템 권한 획득 가능성 완화를 위해 인텔 관리 SKU 클라이언트 언프로비저닝
2. 권한 없는 로컬 공격자의 시스템 권한 획득 가능성 완화를 위해 로컬 관리 서비스(LMS) 비활성화 또는 제거
3. 로컬 관리 구성 제한을 선택적으로 구성

인텔은 네트워크 권한 에스컬레이션 취약성을 해결하기 위해 모든 완화 경로의 첫 번째 단계로 인텔 관리 SKU의 언프로비저닝을 강력히 권장합니다. 프로비저닝된 시스템의 경우, LMS 비활성화 또는 제거 전에 언프로비저닝을 수행해야 합니다. 업데이트된 인텔 관리 SKU 펌웨어의 가용성 보류로, 인텔은 LMS 제거 또는 비활성화를 통한 로컬 권한 에스컬레이션의 완화를 강력히 권장합니다. 선택적으로, 부주의한 LMS 재설치 또는 재활성화에 대한 두 번째 보안 레이어로써, OS를 통해 수행한 일부 관리 구성 옵션이 운영 체제(OS)를 통해 추가적으로 비활성화될 수 있습니다; 그러나 이러한 추가 로컬 관리 구성 제한에는 반전 허용 방법에 대한 제약 조건이 있습니다.

참고: AMT 6.0.x는 호스트 기반 프로비저닝/클라이언트 제어 모델을 지원하지 않으며, 결과적으로 로컬 OS 인터페이스의 INTEL-SA-00075 검출 및 완화 도구를 통한 언프로비저닝이 불가능합니다. 관리 펌웨어 6.0.x.x 또는 6.1.x.x를 사용하는 플랫폼의 경우, 인텔 SCS 제품군의 ACUConfig /full을 사용하거나 시스템 MEBx를 통한 완전한 언프로비저닝이 필요합니다.

이 문서에 제공된 완화 단계 구현 관련 지원은 [인텔 고객 지원팀](#)에 문의하십시오; 기술 섹션에서, Intel® Active Management Technology(Intel® AMT)를 선택하십시오.

INTEL-SA-00075 검출 및 완화 도구 사용

INTEL-SA-00075 검출 및 완화 도구란 무엇인가?

로컬 사용자 또는 IT 관리자가 시스템이 인텔 보안 자문 INTEL-SA-00075에 기록된 익스플로이트에 취약한지 확인하는 데 INTEL-SA-00075 검출 및 완화 도구를 사용할 수 있습니다. 도구의 콘솔 버전을 사용하여 완화 단계를 수행할 수 있습니다.

검출 및 완화 도구는 두 가지 버전으로 제공됩니다.

- 한 가지는 실행 시 장치의 하드웨어와 소프트웨어 세부 사항을 검색하여 리스크 평가 표시를 제공하는 대화형 GUI 도구입니다. 시스템의 로컬 평가를 원할 때 이 버전을 권장합니다.
- 다른 한 가지 버전은 리스크 평가 및 권장 완화 단계를 수행할 수 있는 콘솔 실행 파일입니다. 선택적으로 검색 정보를 Windows* 레지스트리 및/또는 XML 파일에 저장할 수 있습니다. 여러 기계 간 대량 검출 및 완화 작업을 원하는 IT 관리자의 경우 이 버전이 더 편리합니다.

INTEL-SA-00075 검출 및 완화 도구 다운로드

INTEL-SA-00075 검출 및 완화 도구 다운로드 패키지는 다음 페이지에서 다운로드할 수 있습니다:

<https://www.intel.com/content/www/kr/ko/support/technologies/000024133.html>.

시스템 요구 사항

- Microsoft Windows* 7, 8, 8.1 또는 10
- 로컬 운영 체제 관리 액세스

도구 설치

대화형 설치

INTEL-SA-00075 Detection and Mitigation Tool.msi를 실행하고 화면의 프롬프트를 따릅니다.

자동 설치

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

이 파일은 INTEL-SA-00075 검출 및 완화 도구를 기본 디렉터리에 설치합니다.

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

도구 제거

대화형 설치

INTEL-SA-00075 Detection and Mitigation Tool.msi를 실행하고 화면의 프롬프트를 따릅니다.

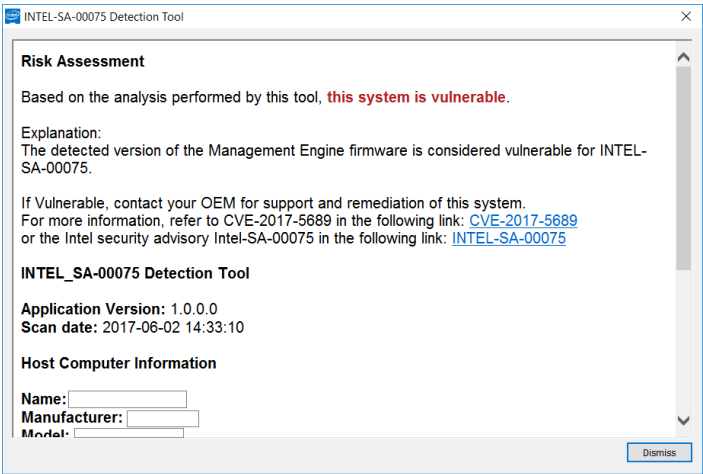
자동 제거

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

GUI 도구 실행

INTEL-SA-00075-GUI.exe 는 단일 시스템에서 실행하도록 설계되었습니다. 실행 시 도구가 검색 정보를 화면에 출력합니다.

그림 1. INTEL-SA-00075-GUI 화면 출력 예시



콘솔 도구 실행

INTEL-SA-00075-console.exe 를 명령 프롬프트에서 관리자 권한으로 실행합니다.

사용법:

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

한 번에 하나의 명령만 실행할 수 있습니다. 명령을 입력하지 않은 경우, 검색 명령이 실행됩니다.

표 1. INTEL-SA-00075 콘솔 명령줄 스위치

명령줄 명령	기능
-Discover	콘솔에 결과를 출력하고 레지스트리에 데이터를 씁니다.
-Unprovision [password], -u [password]	모든 인텔 AMT 설정을 제거하고 인텔 AMT 기능을 비활성화하십시오; 인텔 AMT 장치의 관리 사용자 암호가 사용될 수 있으며 필수일 수도 있습니다. 참고: 암호 없이 이 명령을 호출하는 것은 INTEL-SA-00075(빌드 번호 3000 미만의 6.1.x.x~11.6.x.x)의 영향을 받는 펌웨어 버전에서만 가능합니다. 빌드 번호 3000 이상의 펌웨어 버전 6.1.x.x~11.6.x.x를 사용 중인 경우, 암호를 제공해야 언프로비저닝이 가능합니다.
-DisableClientControlMode, -DisableCCM	인텔 AMT 장치에서 클라이언트 제어 모드 옵션을 영구적으로 비활성화합니다. 이 명령을 실행한 후에는 장치를 클라이언트 제어 모드에 넣을 수 없습니다. 참고: 이 작업을 되돌릴 수 있는 CLI 명령이 없습니다. 경고: 한 번 비활성화된 CCM 을 모든 플랫폼에서 재활성화할 수 있는 것은 아닙니다.
-DisableLMS	LMS 서비스를 비활성화합니다.

명령줄 옵션	기능
-n, -noregistry	레지스트리에 결과를 쓰는 것을 방지합니다
-c, -noconsole	결과가 콘솔에 표시되는 것을 방지합니다
-d, -delay <초>	실행이 시작하기 전 지연 시간(초 단위). 값을 지정하지 않으면 도구가 지연되지 않습니다.
-f, -writefile	결과를 파일에 쓰도록 지정합니다. 파일 이름은 다음 형식을 사용합니다: <컴퓨터 이름>.xml
-p <파일 경로>, -filepath <파일 경로>	출력 파일을 저장할 경로. 경로를 지정하지 않으면 도구가 실행되고 있는 디렉터리에 파일이 쓰여집니다.
-h, -help, -?	이러한 명령줄 스위치 및 해당 기능을 표시합니다

-Discover

검색 명령은 검색 정보를 콘솔에 출력합니다. 또한 기본적으로 레지스트리에 검색 데이터도 씁니다. 콘솔 도구에 명령을 입력하지 않으면 검색 명령이 실행됩니다.

-Unprovision

모든 인텔 AMT 설정을 제거하고 인텔 AMT 기능을 비활성화합니다. 인텔 AMT 장치의 선택적 관리 사용자 암호가 사용될 수 있습니다.

구성된 경우, Intel® AMT 및 ISM 이 컴퓨터 네트워크의 관리 트래픽에 자동으로 수신 대기합니다. 알려진 권한 에스컬레이션 문제에 취약한 시스템은 관리 기능에 대한 승인되지 않은 액세스 방지를 위해 언프로비전 명령을 사용하여 언프로비저닝해야 합니다.

암호 없이 이 명령을 호출하는 것은 INTEL-SA-00075(빌드 번호 3000 미만의 6.1.x.x~11.6.x.x)의 영향을 받는 펌웨어 버전에서만 가능합니다. 빌드 번호 3000 이상의 펌웨어 버전 6.1.x.x~11.6.x.x를 사용 중인 경우, 암호를 제공해야 언프로비저닝이 가능합니다.

-DisableClientControlMode

-DisableClientControlMode 구성 제한은 OS 관리 권한을 얻은 권한 없는 공격자의 완화 반전 방지를 위한 보조 레이어가 필요한 고객을 위한 선택적 단계입니다. 이러한 옵션의 반전은 까다로워 컴퓨터 제조업체가 지원하지 않을 수 있으며 시스템에 대한 물리적 액세스가 필요할 수 있습니다. 이 추가 구성 제한을 수행하려는 경우, LMS 서비스 비활성화 전에 수행해야 합니다.

CCM 재활성화 단계

제조업체에서 지원하는 경우, 인텔 관리 SKU 를 BIOS 에서 재설정할 수 있으며, 이 경우 CCM 이 다시 활성화됩니다. 이 기능의 지원 여부와 따라야 할 절차는 제조업체에 문의하십시오.

참고: 제조업체가 OS 를 통한 BIOS 설정 구성 도구를 제공할 수 있습니다. 이러한 도구를 사용하면 물리적으로 컴퓨터와 접촉할 필요 없이 BIOS 의 인텔 관리 SKU 를 재설정할 수 있습니다. 이 기능을 가진 도구의 제공 여부는 제조업체에 확인하십시오.

-DisableLMS

DisableLMS 명령은 LMS 서비스를 완화 단계로 비활성화합니다.

LMS란 무엇인가?

인텔® 관리 및 보안 애플리케이션 로컬 관리 서비스(LMS)는 일반적인 SOAP 및 WS-관리 기능을 사용하기 위해 Intel® AMT, Intel® SBA 또는 Intel® Standard Manageability 지원 장치에서 실행되는 로컬 애플리케이션을 활성화하는 서비스입니다. 인텔® 관리 엔진(ME) 포트(16992, 16993, 16994, 16995, 623 및 664)에 수신 대기하며 인텔® MEI 드라이버를 통해 트래픽을 펌웨어에 경로 지정합니다.

추가 고려 사항

OS 관리 권한이 있으면 누구나 LMS가 제거된 경우 다시 설치하거나 서비스가 비활성화된 경우 다시 활성화할 수 있습니다. 따라서 시스템에 취약성이 존재하는 동안 부주의한 LMS 재설치 또는 재활성화 방지를 위해 주의하는 것이 중요합니다. 예를 들어, 추후 언젠가 인텔 관리 소프트웨어 설치 관리자를 실행하는 경우 LMS가 다시 설치될 수 있습니다.

그림 2. INTEL-SA-00075-콘솔 출력 예시

INTEL-SA-00075 Discovery Tool

애플리케이션 버전: <앱 버전>

검색 날짜: <날짜 및 시간>

*** 호스트 컴퓨터 정보 ***

컴퓨터 이름: <컴퓨터 이름>

제조업체: <컴퓨터 제조업체>

모델: <컴퓨터 모델>

프로세서: <프로세서 모델>

Windows 버전: <Windows* 버전>

*** ME 정보 ***

버전: <인텔 ME 펌웨어 버전>

SKU: <관리 기능(존재하는 경우)>

상태: <ME 프로비저닝 상태>

설치된 드라이버: <참/거짓>

제어 모드: <없음/ACM/CCM>

CCM 비활성화됨: <참/거짓/알 수 없음>

EHBC 활성화됨 <참/거짓>

LMS 상태: <실행 중/중지됨/존재하지 않음>

LMS 시작 유형: <부팅/시스템/자동/수동/비활성화됨/존재하지 않음>

MicroLMS 상태: <실행 중/중지됨/존재하지 않음>

MicroLMS 시동 유형: <부팅/시스템/자동/수동/비활성화됨/존재하지 않음>

SPS 임: <참/거짓>

*** 리스크 평가 ***

이 도구가 수행한 분석을 기반으로,

< 이 시스템은 취약합니다 /
 이 시스템은 취약하지 않습니다 /
 이 시스템은 취약하지 않습니다; 타사 SKU /
 이 시스템은 취약하지 않습니다; ME FW 버전이 영향을 받지 않습니다 /
 이 시스템은 취약하지 않습니다; ME SKU 가 영향을 받지 않습니다 /
 이 시스템은 취약하지 않습니다; SMBIOS 가 소비자 SKU 임을 나타냅니다 /
 이 시스템은 취약하지 않습니다; 시스템이 SPS FW(서버 플랫폼 서비스 펌웨어)를 실행 중입니다 /
 이 시스템의 펌웨어가 업데이트되었으며 시스템이 언프로비저닝된 상태입니다 /
 이 시스템의 펌웨어가 업데이트되었으며 시스템이 프로비저닝된 상태입니다 /
 OEM 에게 확인하십시오 /
 이 시스템의 리스크를 알 수 없습니다>

취약하다면 OEM 에 연락하여 지원과 이 시스템 복원을 요청하십시오.

*** 추가 정보 ***

다음 웹 페이지에서 CVE-2017-5689 를 참조하십시오:

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

또는 다음 웹 페이지에서 인텔 보안 자문팀 Intel-SA-00075 에 문의하십시오:

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

리스크 평가 확인에 사용된 로직이 표 2 에 설명되어 있습니다.

표 2. 출력의 리스크 평가 의미

메시지	의미
취약함	검색된 관리 엔진 펌웨어 버전이 INTEL-SA-00075 에 취약한 것으로 간주됩니다.
취약하지 않음	8 페이지의 <i>INTEL-SA-00075</i> 검색 도구를 사용하여 영향받은 시스템 식별에 설명된 “취약하지 않음” 기준을 충족하는 시스템.
이 시스템의 펌웨어가 업데이트되었으며 시스템이 언프로비저닝된 상태입니다	이 시스템에서 검색된 펌웨어가 INTEL-SA-00075 에 맞게 수정되었습니다. INTEL-SA-00075 도구가 다시 프로비저닝하기 전에, 시스템의 전체 언프로비저닝을 수행하는 데 사용되었는지 확인하십시오. 이렇게 하면 승인되지 않은 모든 구성 설정이 제거됩니다.
이 시스템의 펌웨어가 업데이트되었으며 시스템이 프로비저닝된 상태입니다	이 시스템에서 검색된 펌웨어가 INTEL-SA-00075 에 맞게 수정되었습니다. 펌웨어 업데이트 전에 시스템이 프로비저닝된 경우, 시스템의 전체 언프로비저닝 및 리프로비저닝이 승인되지 않은 모든 구성 설정이 제거됩니다.
OEM 에 확인하십시오	OEM 의 SMBIOS 에서 검색된 정보가 관리 SKU 를 보여주지만, 컴퓨터로부터 상세 데이터 요청 시 도구가 응답을 수신하지 못했습니다. 이 문제는 관리 엔진 인터페이스 드라이버 누락으로 발생할 수 있습니다. 컴퓨터 모델이 영향을 받는지 여부는 OEM 에 문의하십시오.

메시지	의미
알 수 없음	<p>컴퓨터로부터 하드웨어 인벤토리 데이터 요청 시 도구가 유효한 응답을 수신하지 못했습니다. 이 시스템의 취약성 확인 관련 지원은 시스템 제조업체에 문의하십시오.</p> <p>PMX 드라이버가 설치되지 않은 서버 플랫폼에서 이 메시지를 수신할 수 있습니다. 이 드라이버를 모든 Windows OS 버전에서 사용하지 못할 수도 있습니다. 드라이버가 존재하지 않을 경우, 권장 해결 방법은 SPS 펌웨어 릴리스와 함께 제공된 spsInfo 또는 spsManuf 애플리케이션을 실행하는 것입니다. 두 애플리케이션 모두 PMX 드라이버를 설치합니다.</p>

결과

참고: INTEL-SA-00075 검색 명령어가 반환하는 데이터의 양은 인텔 관리 드라이버 스택이 시스템에 로드되었는지 여부에 따라 다릅니다. 인텔® 관리 엔진 인터페이스(MEI) 드라이버와 인텔® 관리 및 보안 애플리케이션 로컬 관리 서비스(LMS)가 존재하는 경우, 사용 가능한 상세 데이터의 양이 더 많아집니다. 일부 필드는 제조업체가 지원하지 않을 수 있습니다.

레지스트리 위치

결과 표의 값은 다음 레지스트리 키에서 찾을 수 있습니다.

- 32 비트 운영 체제: HKLM\SOFTWARE\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool
- 64 비트 운영 체제: HKLM\SOFTWARE\WOW6432Node\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool

XML

XML 파일에 결과를 쓰려고 하는 경우, 해당 파일은 INTEL-SA-00075-console.exe 가 실행되는 디렉터리 또는 명령줄 옵션에 지정된 경로에 저장됩니다. 하드웨어 인벤토리, OS, LMS 존재 등의 정보가 포함됩니다. AMT 이 존재하는 경우 검색된 기본 및 사용자 지정 인증서 해시 목록이 포함됩니다. 이 목록은 AMT 저장 내용에 대한 예상 해시 감사에 사용될 수 있습니다.

콘솔 반환 코드

표 3. INTEL-SA-00075 콘솔 반환 코드

번호	의미
0	NOTVULNERABLE (검색 명령이 실행된 경우) STATUS_OK
2	MACHINE_STATE_UNCONFIGURED
30	CLIENT_CONFIG_NOT_SUPPORTED

번호	의미
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

표 4. INTEL-SA-00075 콘솔 출력 값

값	위치	설명
Application Version (애플리케이션 버전)		사용되는 검색 도구 버전
Scan Date (검색 날짜)		검색이 수행된 날짜 시간
Computer Name (컴퓨터 이름)		검색한 컴퓨터 이름
Computer Manufacturer (컴퓨터 제조업체)		컴퓨터 제조업체
Computer Model (컴퓨터 모델)	하드웨어 인벤토리	컴퓨터 모델
Processor (프로세서)		컴퓨터의 프로세서 모델
ME Version (ME 버전)		다음 형식의 전체 ME 펌웨어 버전 번호 포함 문자열 값. Major.Minor.Hotfix.Build
ME SKU	ME 펌웨어 정보	존재하는 경우, 시스템의 관리 기능
ME Provisioning State (ME 프로비저닝 상태)		ME 구성 상태 검색되지 않음 프로비저닝되지 않음 프로비저닝 진행 중 프로비저닝됨
ME Driver Installed (ME 드라이버 설치됨)		MEI 드라이버가 컴퓨터에 존재하는 경우 참/거짓 값
EHBC Enabled (EHBC 활성화됨)		시스템에서 포함된 호스트 기반 구성 프로비저닝 방법이 가능한 경우 참/거짓 값
LMS state (LMS 상태)		LMS 서비스 상태가 실행 중, 실행 중이 아님 또는 존재하지 않음 중 무엇인지에 관한 정보
LMS startup type (LMS 시작 유형)		LMS 시작 유형이 존재하지 않음, 부팅, 시스템, 자동, 수동 또는 비활성화됨 중 무엇인지에 관한 정보
MicroLMS state (MicroLMS 상태)		MicroLMS 서비스 상태가 실행 중, 실행 중이 아님 또는 존재하지 않음 중 무엇인지에 관한 정보
MicroLMS startup type (MicroLMS 시작 유형)		MicroLMS 시작 유형이 존재하지 않음, 부팅, 시스템, 자동, 수동 또는 비활성화됨 중 무엇인지에 관한 정보
Control Mode (제어 모드)		ME 구성 모드 없음, ACM 또는 CCM

Is CCM Disabled (CCM 비활성화 여부)		클라이언트 제어 모드의 비활성화에 대한 참/거짓/알 수 없음 상태
Is SPS (SPS 여부)		플랫폼이 취약하지 않은 서버 플랫폼 서비스(SPS) 시스템인가?
*** 리스크 평가 ***	리스크 평가	표 2 참조. <i>출력의 리스크 평가 의미</i>

INTEL-SA-00075 검색 도구를 사용하여 영향받은 시스템 식별

영향받은 시스템은 영향받은 인텔® 관리 엔진(ME) 펌웨어 버전을 가지고 표 5에 정의된 세 가지 관리 기능 세트 중 하나를 포함하는 것으로 정의됩니다.

참고: 서버 플랫폼 서비스(SPS) 플랫폼은 INTEL-SA-00075에 취약하지 않습니다. SPS 플랫폼은 서버 플랫폼의 관리 엔진(ME, PCH의 일부)에서 실행되는 펌웨어를 가집니다. 이 펌웨어는 (동일하게 ME에서 실행되는) PC/워크스테이션 플랫폼의 인텔 관리 펌웨어와는 다릅니다.

표 5. INTEL-SA-00075 검색 도구를 사용한 시스템의 INTEL-SA-00075 취약성 여부 확인 기준

값 이름	취약함	취약하지 않음
ME SKU	인텔® 전체 AMT 관리 인텔® 표준 관리 기능 Intel® Small Business Advantage(SBA)	ME SKU 값이 좌측 취약 목록에 존재하지 않음 - 또는 - 취약하지 않은 펌웨어 버전을 포함한 좌측의 ME SKU 값
ME 버전	3000 미만의 빌드 값을 가진 ME 버전 6.x.x.x~11.7.x.x 예: 9.5.22. <u>1760</u>	ME 버전: <ul style="list-style-type: none"> 3000 이상의 빌드 값을 가진 6.x.x.x~11.7.x.x <ul style="list-style-type: none"> 예: 11.6.27.<u>3264</u> 2.x.x.x. – 5.x.x.x 11.7.x.x 이상

참고: Intel® Small Business Technology(SBT)는 Intel® Small Business Advantage에 대한 관리 SKU입니다.

INTEL-SA-00075 콘솔 도구 결과를 포함하기 위한 Microsoft* SCCM 하드웨어 인벤토리 확장

Intel-SA-00075 콘솔 도구의 결과를 Windows 레지스트리에 저장하려는 경우, Microsoft* SCCM 하드웨어 인벤토리 확장을 활용하여 결과를 가져올 수 있습니다. 따라서 SCCM 에 컬렉션을 구축하여 컴퓨터를 대상으로 한 업데이트 관리 또는 펌웨어 업데이트가 가능해집니다. 이를 위해서는 다음을 수행해야 합니다.

1. 하드웨어 인벤토리 클래스를 SCCM configuration.mof 파일에 추가합니다.
2. 클라이언트 구성에서 이러한 새 하드웨어 인벤토리 클래스를 활성화합니다.
3. 배포할 소프트웨어 패키지를 생성하고 INTEL-SA-00075 콘솔 도구(Intel-SA-00075-console.exe)를 실행합니다.
4. 소프트웨어 패키지 실행 순서를 생성합니다.

MOF 파일 수정

참고: 중앙 서버가 있는 환경에서는 해당 위치에서 MOF 파일을 변경합니다. 또는 모든 기본 서버에서 이러한 사항을 변경합니다.

1. configuration.mof 파일을 찾습니다. 일반적으로 \Program Files\Microsoft Configuration Manager\inboxex\clfiles.src\hinv\에서 찾을 수 있습니다.
2. 백업 복사본을 만듭니다.
3. configuration.mof 파일을 편집하고, 파일 끝까지 아래로 스크롤하여 다음 열 위에 커서를 위치시킵니다.

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

4. 13~14페이지의 MOF 파일 변경사항을 이 문서 3단계의 선 위에 붙여넣습니다.
5. 저장 후 파일을 닫습니다.
6. configuration.mof가 포함된 디렉터리에서 관리자로 실행되는 명령 프롬프트를 시작합니다.
7. 수정된 configuration.mof 파일을 대상으로 하는 스위치 없이 mofcomp를 실행합니다.

하드웨어 인벤토리 변경사항

참고: 생성된 후, 새로운 해당 항목이 하드웨어 인벤토리에 나타나기 전 이러한 변경사항이 클라이언트에 적용될 시간이 필요합니다. 이에 걸리는 시간은 환경이 어떻게 구성되었는지에 따라 다릅니다.

1. INTEL-SA-00075.mof라는 이름의 새 파일을 생성합니다.
2. 185페이지 INTEL-SA-00075 하드웨어 인벤토리 가져오기의 내용을 새로 생성한 파일에 붙여넣고 저장합니다.
3. 구성 관리자 콘솔을 시작합니다.
4. 관리 > 클라이언트 설정 > 기본 클라이언트 설정.
5. 기본 클라이언트 설정 마우스 오른쪽 단추 클릭 > 속성.
6. 하드웨어 인벤토리 선택 > 클래스 설정.
7. 가져오기를 클릭합니다.
8. INTEL-SA-00075.mof 파일로 이동해서 엽니다.
9. “하드웨어 인벤토리 클래스 및 하드웨어 인벤토리 클래스 설정 모두 가져오기” 옵션이 선택되어 있는지 확인합니다.
10. 가져오기를 클릭합니다.
11. 확인, 확인을 클릭합니다.

12. SCCM은 dataldr.log 파일 내 하드웨어 인벤토리의 변경사항을 기록합니다.

SCCM 패키지 생성

1. 15페이지의 배치 파일을 만든 후 INTEL-SA-00075 콘솔 도구 파일을 포함한 폴더에 위치시킵니다.
2. 구성 관리자 콘솔을 시작합니다.
3. 소프트웨어 라이브러리 > 패키지.
4. 패키지 마우스 오른쪽 단추 클릭 > 패키지 만들기.
5. 이름: Intel-SA-00075.
6. 소스 파일이 포함된 이 패키지를 선택합니다.
7. 1단계의 패키지 폴더를 찾습니다.
8. 다음.
9. 프로그램은 만들지 않음을 선택합니다.
10. 다음 > 다음 > 닫기.
11. 적절한 배포 지점에 패키지 배포.

SCCM 작업 순서 생성

1. 구성 관리자 콘솔을 시작합니다.
2. 소프트웨어 라이브러리 > 운영 체제.
3. 작업 순서 마우스 오른쪽 단추 클릭 > 작업 순서 만들기.
4. 새 사용자 지정 작업 순서 만들기를 선택합니다.
5. 다음.
6. Intel-SA-00075의 이름을 입력합니다.
7. 다음 > 다음 > 닫기.
8. Intel-SA-00075 작업 시퀀스를 마우스 오른쪽 단추로 클릭하고 편집을 클릭합니다.
9. 추가 > 일반 > 명령줄 실행.
10. Intel-SA-00075.bat를 명령줄 필드에 입력합니다.
11. 패키지 상자를 선택한 후 검색을 선택합니다.

12. 이전에 생성한 Intel-SA-00075 패키지 선택 > 확인.

13. '확인'을 클릭합니다.

인텔® SCS 시스템 검색 유틸리티 사용

인텔® SCS 시스템 검색 유틸리티는 무엇일까요?

인텔® SCS 시스템 검색 유틸리티는 인텔® 설정 및 구성 소프트웨어(인텔® SCS) 제품군의 구성요소이며 Intel® Active Management Technology(Intel® AMT), Intel® Standard Manageability(ISM) 또는 Intel® Small Business Technology(인텔® SBT)을 지원하는 시스템의 하드웨어 및 소프트웨어에 대한 세부 정보를 제공합니다. 실행 시, Microsoft Windows 레지스트리 및/또는 XML 파일에 결과를 저장할 수 있습니다. 펌웨어 업데이트 대상으로 삼을 시스템을 찾을 때나 완화를 구현할 때 이 정보를 사용할 수 있습니다.

인텔® SCS 시스템 검색 유틸리티 다운로드

인텔® SCS 시스템 검색 유틸리티 다운로드 패키지는 다음 페이지에서 다운로드할 수 있습니다:

<https://downloadcenter.intel.com/download/26691/Intel-SCS-System-Discovery-Utility>.

인텔® SCS 시스템 검색 유틸리티를 사용한 관리 펌웨어 버전 확인

인텔® SCS 시스템 검색 유틸리티의 출력을 시스템의 펌웨어 버전 및 시스템이 관리 SKU 인지 여부를 확인하는 데 사용할 수 있습니다 이 정보는 출력의 ManageabilityInfo 섹션에서 제공됩니다. 도구 실행 관련 지침은 12 페이지의 *인텔® SCS 시스템 검색 유틸리티 실행* 섹션을 읽어보십시오.

FWVersion 값은 현재 장치에 있는 펌웨어 버전을 포함합니다. AMTSSKU 값은 지원되는 관리 SKU 를 포함합니다(존재하는 경우). FWVersion 및 AMTSKU 의 값을 검토하여 표 6 에 따라 시스템의 취약성을 확인하십시오.

표 6. 인텔® SCS 시스템 검색 유틸리티를 사용한 시스템의 INTEL-SA-00075 취약성 판단 기준

값 이름	취약함	취약하지 않음
AMTSKU	Intel(R) Full AMT Manageability Intel(R) Standard Manageability Intel(R) Small Business Advantage(SBA) 출력 예: <ManageabilityInfo> <AMTSKU>Intel(R) Full AMT Manageability</AMTSKU> <AMTversion>11.0.0</AMTversion> <FWVersion>11.0.0.1202</FWVersion>	출력에 존재하지 않는 AMTSKU 값 - 또는 - 취약하지 않은 펌웨어 버전을 포함한 좌측의 AMTSKU 값 출력 예: <ManageabilityInfo> <FWVersion>9.0.13.1402</FWVersion>

FWVersion	3000 미만의 빌드 값을 가진 인텔® 관리 SKU 펌웨어 버전 6.x.x.x~11.7.x.x 예: 9.5.22. <u>1760</u>	인텔® 관리 SKU 펌웨어 버전: <ul style="list-style-type: none"> 3000 이상의 빌드 값을 가진 6.x.x.x~11.7.x.x <ul style="list-style-type: none"> 예: 11.6.27.<u>3264</u> 2.x.x.x. – 5.x.x.x 11.7.x.x 이상
-----------	---	---

참고: Intel® Small Business Technology(SBT)는 Intel® Small Business Advantage 에 대한 관리 SKU 입니다.

인텔® SCS 시스템 검색 유틸리티 실행

레지스트리에만 데이터 저장

인텔® 시스템 SCS 검색 유틸리티를 실행하고 레지스트리에 데이터를 쓰기 위해 관리 권한을 가진 명령 프롬프트로부터 다음 명령을 실행하십시오.

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

XML 파일에만 데이터 저장

인텔® SCS 시스템 검색 유틸리티를 실행하고 XML 파일에 데이터를 저장하기 위해 다음 명령을 사용하십시오.

```
SCSDiscovery.exe SystemDiscovery <파일 이름 및 경로> /noregistry
```

파일 이름과 경로는 시스템 또는 네트워크 공유의 로컬 위치일 수 있습니다. 네트워크 공유를 사용하려는 경우, 인텔® SCS 시스템 검색 유틸리티를 실행하는 계정이 해당 네트워크 공유에 대한 쓰기 권한을 가지고 있는지 확인하십시오. 파일 이름과 경로를 지정하지 않을 경우, XML 파일 이름에 시스템의 FQDN이 사용되며 파일이 인텔® SCS 시스템 검색 유틸리티를 포함하는 디렉터리에 저장됩니다.

레지스트리 및 XML 파일에 데이터 저장

인텔® SCS 시스템 검색 유틸리티를 실행하여 레지스트리 및 XML 파일에 데이터를 저장하기 위해 다음 명령을 사용하십시오

```
SCSDiscovery.exe SystemDiscovery <파일 이름 및 경로>
```

이전 예제와 같이, 파일 이름과 경로를 지정하지 않을 경우, XML 파일 이름에 시스템의 FQDN이 사용되며 파일이 인텔(R) SCS 시스템 검색 유틸리티를 포함하는 디렉터리에 저장됩니다.

인텔® SCS 시스템 검색 유틸리티의 결과

인텔® SCS 시스템 검색 유틸리티가 반환하는 데이터의 양은 인텔 관리 드라이버 스택이 시스템에 로드되었는지 여부에 따라 다릅니다. 인텔® 관리 엔진 인터페이스(MEI) 드라이버와 인텔® 관리 및 보안 애플리케이션 로컬 관리 서비스(LMS)가 존재하는 경우, 사용 가능한 상세 데이터의 양이 더 많아집니다. 아래 설명된 결과는 알려진 권한 에스컬레이션 문제와 관련된 일부 주요 데이터 필드에만 초점을 맞춥니다. 다른 데이터 필드 관련 추가 세부 사항은 인텔® SCS 시스템 검색 유틸리티 문서를 참조하십시오. 일부 필드는 제조업체가 지원하지 않을 수 있습니다.

레지스트리 결과

레지스트리에 저장된 결과는 다음 위치에서 찾을 수 있습니다.

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

키 값:

값 이름	레지스트리 하위 키	값 설명
FWVersion	ManageabilityInfo	인텔® 관리 엔진 펌웨어 버전
AMTSKU	ManageabilityInfo	지원되는 관리 기능(존재하는 경우)

XML 파일 결과

인텔® 관리 엔진 펌웨어 버전은 XML의 다음 경로에서 찾을 수 있습니다.

```
<SystemDiscovery>
  <ManageabilityInfo>
    <FWVersion> 버전 번호 </FWVersion>
```

시스템의 지원되는 관리 기능(존재하는 경우)은 XML의 다음 경로에서 찾을 수 있습니다.

```
<SystemDiscovery>
  <ManageabilityInfo>
    <AMTSKU> 관리 기능 이름 </AMTSKU>
```

SCCM 하드웨어 인벤토리로 시스템 검색 데이터 가져오기

Microsoft* System Center Configuration Manager(SCCM)용 인텔® SCS 추가 기능을 통해 시스템 검색 데이터 수집 프로세스를 자동화할 수 있습니다. 설치 시, 이 추가 기능이 SCCM 하드웨어 인벤토리를 자동 확장하여 시스템 검색 데이터를 포함함과 동시에 시스템 컬렉션에 대한 시스템 검색 실행에 사용될 수 있는 작업 순서를 생성합니다. 그런 뒤 이 프로세스를 통해 수집된 정보는 영향을 받은 시스템에 펌웨어 업데이트 또는 완화를 푸시하기 위한 SCCM 컬렉션 생성에 사용될 수 있습니다.

Microsoft SCCM 용 인텔® SCS 추가 기능 다운로드 패키지는 다음 페이지에서 다운로드할 수 있습니다:

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

MOF 파일 변경사항

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

INTEL-SA-00075 하드웨어 인벤토리 가져오기

```
#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_I
nformation"),
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 배치 파일

```
@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%
```

컬렉션 쿼리 샘플

프로비저닝된 컴퓨터

```
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 실행

```
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"
```

여기에 포함된 모든 정보는 인텔® 제품과 함께 제공됩니다. 이 문서를 제공한다고 해서 금반언이나 기타 다른 방법으로 지적 재산권에 대한 명시적 또는 묵시적 라이선스를 부여하는 것은 아닙니다. 그러한 제품에 대해서는 인텔의 판매 규약과 조건에 제공된 사항을 제외하고, 인텔은 어떠한 책임도 지지 않으며 특정 용도예의 적합성이나 상업성 또는 특허권이나 기타 지적 재산권의 침해에 관한 책임이나 품질 보증을 포함하여 인텔 제품의 판매 및/또는 사용과 관련하여

어떠한 명시적 또는 묵시적인 보증도 하지 않습니다. 인텔에서 서면으로 동의하지 않는 한, 인텔 제품은 인텔 제품의 장애가 개인 부상이나 사망을 유발하는 상황을 초래할 수 있는 응용 분야용으로 설계되지도, 그러한 경우에 사용하도록 의도되지도 않았습니다.

인텔 기술의 기능 및 이점은 시스템 구성에 따라 달라지며 지원되는 하드웨어, 소프트웨어 또는 서비스 활성화가 필요할 수 있습니다. 성능은 시스템 구성에 따라 달라집니다. 어떠한 컴퓨터 시스템도 절대적으로 안전하지는 않습니다. 시스템 제조업체 또는 소매점을 통해 확인하거나 intel.co.kr 에서 자세한 내용을 알아보십시오.

Copyright © 2017 Intel Corporation. 모든 권리 보유. 인텔 및 인텔 로고는 미국 및/또는 기타 국가에서 인텔사의 상표입니다.

* 다른 이름과 상표명은 각 소유주가 재산을 주장할 수 있습니다.