ホワイトペーパー

INTEL-SA-00075 問題緩和ガイド

インテル®アクティブ・マネジメント・テクノロジー (インテル® AMT) は、インテル®スタンダード・マネージャビリティー (ISM) インテル®スモール・ビジネス・テクノロジー (スモール・ビジネス・テクノロジー) 。

INETL-SA-00075に記載されている
セキュリティー脆弱性問題を緩和する方法

バージョン 1.2-2017 年 5 月 5 日

目次

エグゼクティブ・サマリー

このドキュメントは、Intel Management SKU System 上で起こりうる、権限昇格問題として知られているセキュリティ上の脆弱性を緩和する方法を提供します。詳細については、パブリックセキュリティーアドバイザリーをご参照ください。
https://security-center.intel.com/advisory.aspx?intelid=INTEL-sa-00075&languageid=en-fr

これらの問題を緩和する方法は、脆弱性に対処したファームウェアが適用されていない Intel Management SKUs、インテル®アクティブ・マネジメント・テクノロジー (インテル® AMT)、インテル®スタンダード・マネージャビリティー (ISM) 、およびインテル®スモール・ビジネス・テクノロジー (スモール・ビジネス・テクノロジー)に対し、無許可の有効化ならびに使用を防ぐことです。

IT 専門家は、管理コンソール内でこれらのスクリプトとタスクを使って緩和策を広範囲に適用できます。緩和策の実施手順は以下の通りです。

1. Intel Management SKUクライアントをアンプロビジョンすることで、権限を持っていないネットワーク攻撃者によるシステム権限取得を防止する
2. Local Manageability Service(LMS)を無効化または削

除することで、権限を持っていないローカル攻撃者によるシステム権限取得を防止する

3. オプションでローカル管理機能設定の制限を設定する

インテルは、ネットワークの権限昇格問題のすべての緩和策の最初のステップとして、Intel Management SKU をアンプロビジョンすることを強く推奨します。プロビジョンされたシステムに対しては、LMS を無効化または削除する前に、必ずアンプロビジョンする必要があります。（この問題が対処された）Intel Management SKU 用のファームウェアの配布を待っている間、ローカルの権限昇格問題に対処するため、インテルは LMS の無効化または削除を強く推奨します。追加措置として、意図しない LMS の再インストールおよび再度有効化に対抗するために、OS の管理機能の設定の一部を OS 経由で無効化することができます。ただし、これらのローカル管理設定の追加による制限は、すでにある許可設定と競合するかもしれません。

この文書で提供されている緩和策を実装する際のサポートは、インテル・カスタマー・サポートに問い合わせてください。問い合わせの際は、テクノロジーセクションから、インテル®アクティブ・マネジメント・テクノロジー（ インテル® AMT）を選択してください。

ステップ 1: クライアントのアンプロビジョン

設定時、インテル® AMT と ISM は、コンピューターネットワークのマネジメントトラフィックをリスンします。権限昇格問題を持つとわかっているシステムは、ツールをつかって権限を持たないマネジメント機能へのアクセスを防止するよう初期設定し、アンプロビジョンするべきです。例として、Intel Setup and Configuration Software(Intel SCS) にあるインテル® AMT configuration Utility(ACUConfig)をダウンロードし、コマンドラインで実行することで、システムをアンコンフィギュアすることができます。

アンコンフィギュアコマンドの例（これらの実行には OS 管理者権限が必要です）

CCM に設定されているシステムのアンコンフィギュア ：

```
ACUConfig.exe UnConfigure
```

RCS 利用なしの ACM に設定されているシステムのアンコンフィギュア ：

```
ACUConfig.exe UnConfigure /AdminPassword
<password> /Full
```

RCS 利用のシステムのアンコンフィギュア

```
ACUConfig.exe UnConfigure /RCSaddress
<RCSaddress> /Full
```

詳細については、インテル® SCS のユーザガイドのセクション 6.14 Unconfiguring インテル® AMT systems を参照してください。
Intel SCS と ACUConfig は、次の URL からダウンロードできます。：
http://www.intel.com/go/scs

代替アンプロビジョンツール

前述手順を実行することができない場合は、代替として、投稿された 「INTEL-SA-00075 Unprovisoning Tool」を参照し、アンプロビジョンしてください。

次に、緩和策を終わらせるため、以下のステップ２に進んでください。

ステップ 2:LMS の削除や無効化

注: クライアントのアンプロビジョンや OS からの Intel Management SKU の設定制限は、LMS の実行状況に依存します。これらのステップは、LMS の削除または無効化より前に実行してください。

LMS とは何か

Intel ® Management and Security Application Local Management Service(LMS)は、インテル® AMT、Intel SBA または Intel Standard Manageabilityをサポートしているデバイス上でローカルアプリケーションが、SOAPとWS-Management技術を使うことを可能にするサービスです。LMSは、Intel Management Engine (ME)のためにポート（16992,16993,16994,16995,632と664）をリスンし、トラフィックをIntel MEIドライバを介してファームウェアへルーティングします。

LMS を無効化する手順

注: Service Control Manager と 通信するために Windows に組みこまれているコマンドラインプログラム SC を使います。ActiveDirectory Group Policy Object(GPO)でも LMS の広範囲な無効化が可能です。

コマンドプロンプトから、下記のコマンドを管理者権限で実行します。

```
SC Config LMS start=disabled
```

LMS を削除する手順

コマンドプロンプトから、下記のコマンドを管理者権限で実行します。

```
sc delete LMS
```

注 ： このコマンドは Windows サービスから LMS を削除します。システムから LMS を完全に削除するには、実行可能な lms.exe も削除する必要があります。パスが分からない場合は、コマンドプロンプトから次のコマンドを実行して検索することができます。

```
SC QC LMS
```

その他の注意事項

OS の管理者権限を持つすべてのユーザーは、 LMS が削除された場合でも、LMSを再インストールすることができ、また無効化されている場合は、再度有効化できます。これはこの緩和策の弱点ではありません。なぜなら、これらの事は、今回の脆弱性問題がなくてもOSの管理者権限を持つすべてのユーザーが実行可能なことだからです。関連して重要なことですが、脆弱性のあるシステムに対して、LMSの意図しない再インストールや再度有効化は防止すべきです。例えば、将来、Intel Management softwareインストーラーを実行した際、LMSが再インストールされるかもしれないからです。

代替 LMSとは

管理コンソールエージェントは、Intel Management SKUを管理するために、代替LMSを含むことがあります。１つの例はMicroLMSで、これはMeshCentralオープンソースプロジェクトのコンポーネントの１つです。

ローカルLMSが有効であるかを確認する

Local Management Service (LMS) と MicroLMS のような亜種が適切に無効化されているかどうかは、Intel ME の Internet Assigned Names Authority(IANA)のポート 16992、16993、16994、16995、623 と 664 をリスンするソケットがないことで確認できます。

以下 Windows のコマンドは、Intel ME IANA ポートをリスンしているアプリケーションがあるかどうかを調べます。

```
netstat -na | findstr "\<16993\> \<16992\>
\<16994\> \<16995\> \<664\> \<623\>"
```

注 ： これらは LMS では標準的に使われるポートですが、別のポートをリスンする LMS を開発することも可能です。

オプションの手順 ： ローカル管理機能の構成設定の制限

注 ： このセクションで説明されている設定制限は、権限を持たない攻撃者が OS の管理者権限を持って緩和策に逆行しようとすることに対する追加措置を必要とされるお客様に対するオプションのステップです。これらの追加措置に対する逆行は困難で、コンピューターの製造元によってサポートされていないかもしれず、物理的なシステムへのアクセスが必要かもしれません。もしこの設定の制限を追加するなら、LMS の無効化の前におこなわなければなりません。

ACUConfigによるCCM の無効化手順

クライアント・コントロール・モード(CCM)を、インテル®セットアップ・アンド・コンフィギュレーション・ソフトウェア （ インテル® SCS) のコンポーネントである ACUConfig を用いて無効化することができます。インテル® SCS は次の URL から入手できます。

http://www.intel.com/go/scs

CCM は、管理者権限を持つユーザーは、コマンドプロンプトから次のコマンドを使用して無効にすることができます。

```
ACUConfig.exe DisableClientControlMode
```

確認プロンプトの抑制は、コマンドラインスイッチ、/confirmDisableCCM を用いて実行できます。詳細はインテル® SCS のユーザガイドセクション 6.16 Disabling Client Control Mode を参照してください。

CCM を再度有効にする手順

製造元がサポートしている場合、Intel Management SKU を BIOS からリセット、CCM を再度有効化できることがあります。この機能がサポートされているかどうかは、製造元に問い合わせてください。

注：製造元は BIOS の設定を OS から変更できるツールを提供することがあります。もしこういったツールが提供されているなら、物理的に対象となるコンピュータに触れることなく Intel Management SKU を BIOS からリセットできるかもしれません。このツールの存在と機能については、製造元に問い合わせてください。

EHBC を ACUConfigで無効化する手順

Embedded Host Based Configuration (EHBC) をサポートしてるプラットフォームは、ACUConfig でそれを無効化できます。これは永続的な変更で、コンピュータの製造元のサポートなしで元に戻すことはできません。

EHBC は、管理者権限を持つユーザーは、コマンドプロンプトから次のコマンドを使用して無効にすることができます。

```
ACUConfig.exe DisableEmbeddedHBC
```

詳細については、インテル® SCS のユーザガイドのセクション 6.18 Disabling the EHBC Option を参照してください。

この文書の情報はインテル® 製品との関連で提供されています。本資料は、明示されているか否かにかかわらず、また禁反言によるとよらずにかかわらず、いかなる知的財産権のライセンスを許諾するためのものではありません。は、かかる製品の販売しているインテルの利用規約がでている場合を除き、インテルはいかなる責任はありません、およびインテルは、明示または黙示を問わず、一切の保証、責任を含むインテル製品の販売および / または使用に関連する、または特定目的への、商品性、または侵害に関連する保証のあらゆる特許権、著作権またはその他の知的所有権。インテルが書面で同意した場合を除き、インテル製品はそのインテル製品の障害によって人身事故や死亡事故が引き起こされうるような用途に対して設計されておらず、そのような使用は意図されていません。

インテル・テクノロジーの機能と利点をシステム構成に依存して有効になっているハードウェア、ソフトウェア、またはサービスの有効化が必要になることもあります。実際の性能はシステム構成に応じて異なります。絶対安全なコンピューター・システムはありません。Intel.com または詳細についてはシステム製造元または販売店にお問い合わせください。

* その他の社名、製品名などは、一般に各社の表示、商標または登録商標です。