Symantec SYMSA-2006-003 Cisco Secure ACS for Windowsへの応答：管理者パスワードの開示

Informational

アドバイザリーID : cisco-sa-20060508-acs
初公開日 : 2006-05-08 21:30
バージョン 1.0 : Final
回避策 : No Workarounds available
Cisco バグ ID :

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

これは、2006年5月8日に公開されたSymantecのアドバイザリSYMSA-2006-003に記載されている記述に対するCisco PSIRTの回答です。

元の電子メール/アドバイザリは、http://www.symantec.com/enterprise/research/SYMSA-2006-003.txtで入手できます。

この問題は、Cisco Bug ID:

- CSCsb67457(登録ユーザ専用):Cisco Secure ACS Administrator Password Remote Retrieval and Decryption。

この脆弱性を報告していただいたAndreas Junestam氏とSymantec氏に感謝いたします。

Cisco では、研究者と協力してセキュリティ脆弱性に関する調査を進め、製品レポートで発表することを常に歓迎しています。

追加情報

Cisco Secure Access Control Server(ACS)は、シスコデバイスに対して一元化されたID管理とポリシー適用を提供します。

CSCsb67457(登録ユーザ専用):Cisco Secure ACS Administrator Password Remote Retrieval and Decryption。

症状：

Cisco Secure ACS 3.x for Windowsを実行しているシステムのWindowsレジストリへの管理アクセス権を持つユーザは、すべてのACS管理者のパスワードを復号化できます。

[Condition]：

Cisco Secure ACS 3.x for Windowsは、ACS管理者のパスワードを暗号化形式でWindowsレジストリに保存します。ローカルで生成されたマスターキーは、ACS管理者パスワードの暗号化/復号化に使用されます。マスターキーは、Windowsレジストリにも暗号化形式で保存されます。Microsoftの暗号化ルーチンを使用すると、Cisco Secure ACSを実行しているシステムに対する管理者権限を持つユーザが、マスターキーのクリアテキストバージョンを取得できます。マスターキーを使用すると、ユーザは復号化して、すべてのACS管理者のクリアテキストパスワードを取得できます。Cisco Secure ACSに対する管理者クレデンシャルを使用すると、ローカルに定義されたユーザのパスワードを変更できます。これは、認証にCisco Secure ACSを使用するように設定されたネットワークデバイスにアクセスするために使用できます。

Cisco Secure ACSを実行しているシステムでリモートレジストリアクセスが有効になっている場合、管理者権限を持つユーザ（通常はドメイン管理者）がこの脆弱性を不正利用する可能性があります。

Cisco Secure ACSがWindows Active Directory/ドメインまたはLDAPなどの外部認証サービスを使用するように設定されている場合、これらのサービスによって保存されるユーザのパスワードは、この脆弱性によって危険にさらされることはありません。

この脆弱性の影響を受けるのは、Cisco Secure ACS for Windowsのバージョン3.xだけです。Cisco Secure ACS for Windows 4.0.1およびCisco Secure ACS for UNIXには脆弱性はありません。Cisco Secure ACS 3.xアプライアンスは、ローカルまたはリモートのWindowsレジストリアクセスを許可しないため、脆弱ではありません。

回避策：

ACS管理者のパスワードを含むレジストリキーへのアクセスを制限することで、この脆弱性を軽減できます。Windowsオペレーティングシステムの機能の1つは、レジストリキーのアクセス許可を変更して、ローカルまたはドメインの管理者のアクセス権を削除する機能です。この機能を使用すると、ACS管理者のパスワードを含むレジストリキーを、ACSのインストールの維持やACSサービスの操作を必要とするWindowsユーザだけに制限できます。

次のレジストリキーとそのすべてのサブキーを保護する必要があります。

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.3\CSAdmin\Administrators

注：レジストリキーパスの「CiscoAAAv3.3」部分は、インストールされているCisco Secure ACS for Windowsのバージョンによって少し異なる場合があります。

Cisco Secure ACSの一般的な導入シナリオは2つあります。レジストリキーへのアクセス許可を

必要とするWindowsユーザーは、展開の種類によって異なります。

- Cisco Secure ACSがWindowsドメインコントローラにインストールされていない場合、レジストリキーへのアクセスは、ローカルのWindows SYSTEMアカウントと、ACSインストールでソフトウェアメンテナンスを実行する特定のローカル/ドメイン管理者だけに制限する必要があります。
- Cisco Secure ACSがWindowsドメインコントローラにインストールされている場合、レジストリキーへのアクセスは、ACSがサービスに使用するように設定されているドメインアカウント、ローカルのWindows SYSTEMアカウント、およびACSインストールでソフトウェアメンテナンスを実行する特定のローカル/ドメイン管理者に制限する必要があります。

Windowsレジストリの編集については、次のMicrosoftのマニュアルを参照してください。

“Microsoft Windowsレジストリの説明":

http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986

Cisco Secure ACS for Windowsを実行しているシステムで、許可されたユーザへのアクセスを制限したり、Windowsレジストリへのリモートアクセスを無効にしたりすることで、リモートからの悪用に対する緩和策を強化できます。リモートレジストリアクセスを制限する方法については、次のMicrosoftのマニュアルを参照してください。

「リモート・コンピュータからレジストリへのアクセスを制限する方法」:

http://support.microsoft.com/kb/q153183

「レジストリへのリモートアクセスの管理方法」:

http://support.microsoft.com/kb/q314837

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060508-acs

改訂履歴

バージョン	説明	セクション	日付
リビジョン 1.0	初回公開リリース		2006年5月8日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。