Application Velocityシステムのデフォルト・パスワード

アドバイザリーID : cisco-sa-20080123-avs CVE-2008-0029
初公開日 : 2008-01-23 16:00
バージョン 1.0 : Final
CVSSスコア : 10.0
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

ソフトウェアバージョンAVS 5.1.0より前のバージョンのCisco Application Velocity System(AVS)では、初期設定プロセスでシステムアカウントパスワードの変更を求めるメッセージは表示されません。初期設定プロセス中にこれらのクレデンシャルを変更する必要がないため、攻撃者はデフォルトのクレデンシャルを持つアカウント（一部はルート権限を持つ）を活用して、AVSシステムの完全な管理制御を取得できる場合があります。

ソフトウェアバージョンAVS 5.1.0にアップグレードすると、ユーザはこれらのクレデンシャルを変更するように求められます。

シスコでは、該当するお客様用に、この脆弱性に対応する無償アップグレードソフトウェアを提供する予定です。ソフトウェアアップグレードは、AVS 3120、3180、および3180Aシステムにのみ適用されます。このドキュメントで確認されている回避策は、AVS 3110のソフトウェアの現在のリリースでパスワードを変更する方法を示しています。

この脆弱性には、Common Vulnerabilities and Exposures（CVE）識別子 CVE-2008-0029 が割り当てられています。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080123-avs で公開されています。

該当製品

脆弱性のある製品

この脆弱性は、AVS 5.1.0より前のソフトウェアバージョンを実行しているCisco AVS 3110、

3120、3180、および3180A Management Stationアプライアンスに影響を与えます。管理者は、管理ステーションのWebベースのユーザー・インターフェイスにログインするか、アプライアンスのオペレーティング・システムのコマンド・ライン・インターフェイス(CLI)からAVSアプライアンスのソフトウェア・バージョンを確認できます。

AVS 3180または3180A管理ステーションをご使用のお客様は、Cluster Information Pageに移動してノードソフトウェアのバージョンを確認できます。登録された各ノードは、ノードが選択されたときに対応するソフトウェアバージョンを表示します。

AVSアプライアンスのバージョンは、ホストのオペレーティングシステムからShow Versionコマンドを使用して確認することもできます。

次の例は、バージョン5.1.0を実行しているAVS 3120アプライアンスでのShow Versionの出力を示しています。

```
<#root>

velocity>

Show Version


****************************************
Cisco Application Velocity System,(AVS)
----------------------------------------
AVS 3120-K9 005.001(000.034)
****************************************
```

次の例は、バージョン5.1.0を実行しているAVS 3180または3180Aアプライアンスでの Show Versionの出力を示しています。

```
<#root>

velocity>

Show Version


****************************************
Cisco Application Velocity System,(AVS)
----------------------------------------
AVS 3180-MGMT 005.001(000.034)
****************************************
```

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

Cisco AVS 3110および3120は、Webアプリケーションのパフォーマンス向上、エンドユーザの応答時間の測定、アプリケーションセキュリティの管理を行うエンタープライズデータセンターアプライアンスです。Cisco AVS 3120は、統合Webアプリケーションファイアウォールを使用してアプリケーションセキュリティを適用します。Cisco AVS 3180および3180A Management Stationは、AVS 3110および3120のクラスタまたは個々のノードの設定およびアプリケーションパフォーマンスモニタリング用のWebベースのツールを提供します。

Cisco AVS 3110、3120、3180、および3180A管理ステーションでは、デフォルトのパスワードで初期設定された一部のシステムアカウントが使用されます。脆弱性のあるバージョンのAVSソフトウェアでは、初期構成プロセス中に、root権限を持つアカウントを含むこれらのアカウントのパスワードを変更するように管理者に求められません。脆弱性のないバージョンのAVSソフトウェアでは、インストール後にこれらのアカウントを変更するよう管理者に求めるメッセージが表示されるようになりました。

注：AVS 3110または3120のパスワードがデバイス自体で変更され、AVS 3180または3180A管理ステーションに登録されている場合は、そのノードを管理ステーションコンソールに再登録する必要があります。そうしないと、AVS 3180または3180A管理ステーションとAVS 3110または3120ノード間の通信が失われます。

AVSノード登録プロセスの詳細については、『Cisco AVSユーザガイド』の「ノードの登録」セクションを参照してください。

アプライアンスソフトウェアをバージョンAVS 5.1.0にアップグレードして初めてログインすると、管理者はシステムアカウントのパスワードを変更するように求められます。

次の例は、アップグレード後のAVS 3120の新しいパスワード変更プロンプトと、それに続くパスワード変更ダイアログを示しています。

```
velocity login: fgn
Password:
**WARNING** System wide secrets are in factory default state.
Would you like to change these now? [y/n] y changing root password
enter password:
enter password again:
changing fgn password
enter password:
enter password again:
changing DB password
enter password:
enter password again:

Please wait...The DB password change will take a few minutes.
changing node manager password
enter password:
enter password again:
changing condenser password
```

```
enter password:
enter password again:
changing console password
enter password:
enter password again:
```

次の例は、アップグレード後のAVS 3180および3180Aの新しいパスワード変更プロンプトと、それに続くパスワード変更ダイアログを示しています。

```
velocity login: fgn
Password:
**WARNING** System wide secrets are in factory default state.
Would you like to change these now? [y/n] y changing root password
enter password:
enter password again:
changing fgn password
enter password:
enter password again:
changing DB password
enter password:
enter password again:

Please wait...The DB password change will take a few minutes.
changing console password
enter password:
enter password again:
```

この問題は、Cisco Bug ID CSCsd94732(登録ユーザ専用)に記載されています。

回避策

次の回避策はAVS 3110にのみ適用され、システムシェルで実行されます。AVS 3110にはCLIがありません。強力なパスワードの使用を推奨します。

ルートパスワードの変更

次のステップを実行します。

1. 次のコマンドを使用して、rootパスワードを変更します。

```
shell# passwd
```

2. 次のコマンドを使用してリブートし、新しい設定をアクティブにします。

```
shell# reboot
```

管理コンソールのユーザー名とパスワードの変更

次のステップを実行します。

1. テキストエディタで次のファイルを開きます。

   $AVS_HOME/console/jboss-3.0.1_tomcat-4.0.4/server/default/deploy/fgconsole.war/users.properties

   ユーザ名とパスワードを設定するには、admin=adminの行を使用します。ユーザ名は等号(=)の前に表示され、パスワードは等号(=)の後に表示されます。たとえば、ユーザ名をCiscoに、パスワードをaccelerateに変更するには、admin=admin行をCisco=accelerateに変更します。

2. ユーザ名を変更する場合は、次のファイルも変更する必要があります。

   $AVS_HOME/console/jboss-3.0.1_tomcat-4.0.4/server/default/deploy/fgconsole.war/roles.properties

   ユーザ名は、admin=を含む行で設定します。ユーザ名は等号(=)の前に表示されます。たとえば、ユーザ名をCiscoに変更するには、admin=の行をCisco=に変更します。このファイルの等号(=)の後のテキストは変更しないでください。このフィールドにはアカウント権限が指定されます。ここで入力するユーザ名は、前の手順でusers.propertiesファイルに保存されているユーザ名と一致している必要があります。

データベースのユーザ名とパスワードの変更

データベースパスワードを変更するには、次の2つの手順を実行する必要があります。

1. 最初にデータベースパスワードを変更します。
2. 次に、管理コンソールの設定ファイルを新しいデータベースパスワードで更新します。

次のステップを実行します。

1. 古いパスワードを使用してデータベースにログインし、alter SQLコマンドを使用して新しいパスワードに変更します。

```
/usr/local/fineground/console/postgres/bin/psql
         -U fineground -p 5432 fgnlog Password : <old password>
Welcome to psql 7.3.4, the PostgreSQL interactive terminal.
```

```
Type:  \copyright for distribution terms
       \h for help with SQL commands
       \? for help on internal slash commands
       \g or terminate with semicolon to execute query
       \q to quit
fgnlog=# alter user fineground password '<new password>'; \q
```

2. 管理コンソールのデータベースにアクセスするためのユーザー名とパスワードは、管理コンソールのインストール・プロセス中に設定します。これらの設定を後で変更する場合は、管理コンソール・サーバーが起動時に読み取るXML構成ファイルを変更できます。

   a. テキストエディタで次のファイルを開きます。

      $AVS_HOME/console/jboss-3.0.1_tomcat-4.0.4/server/default/deploy/postgres-service.xml

      このファイルで次のセクションを探します。

```
<!--set these only if you want only default logins,
           not through JAAS -->
<config-property name="UserName" type="java.lang.String">fineground</config-property>
<config-property name="Password" type="java.lang.String">condenser</config-property>
```

   b. ユーザ名を変更するには、UserName設定プロパティ(この例ではfineground)の値を変更します。

   c. パスワードを変更するには、パスワード設定プロパティ(この例ではconcentrator)の値を変更します。

   d. ファイルを保存して、閉じます。

ノードマネージャのパスワードの変更

次のステップを実行します。

1. fgnとしてログインし、suコマンドを使用してスーパーユーザに切り替えます。
2. Concentrator and Node Managerを停止します。

```
/etc/init.d/fgnpn<Tab> stop
```

Tabキーを押して、インターフェイスにコマンドを完成させます。

3. $AVS_HOME/perfnode/node_manager/confディレクトリに移動します。
4. passwordsという名前のファイルをバックアップします。
5. 次のコマンドを使用して、パスワードを変更します。

```
$AVS_HOME/perfnode/bin/htpasswd -bcm passwords.new admin <password>
```

上記のコマンドのpasswords.newには、パスワードが保存されているファイルの名前を指定します。現在はユーザadminのみがサポートされています。

6. 次のコマンドを使用してファイルをインストールします。

```
install -m 400 -o nobody -g nobody passwords.new  passwords
```

7. rebootコマンドを使用して、アプライアンスを再起動します。
8. ノード・マネージャのパスワードが変更されたノードを管理コンソールから再登録します。

コンデンサのパスワードの変更

次のステップを実行します。

1. fgnとしてログインし、suコマンドを使用してスーパーユーザに切り替えます。
2. Concentrator and Node Managerを停止します。

```
/etc/init.d/fgnpn<TAB> stop
```

Tabキーを押して、インターフェイスにコマンドを完成させます。

3. $AVS_HOME/perfnode/passwdディレクトリに移動します。
4. .htpasswdという名前のファイルをバックアップします。
5. 次のコマンドを使用して、パスワードを変更します。

```
$AVS_HOME/perfnode/bin/htpasswd -bcm passwords.new fineground <password>
```

上記のコマンドのpasswords.newには、パスワードが保存されているファイルの名前を指定します。現在は、ユーザfinegroundだけがサポートされています。

6. 次のコマンドを使用してファイルをインストールします。

```
install -m 400 -o nobody -g nobody passwords.new  .htpasswd
```

7. rebootコマンドを使用して、アプライアンスを再起動します。
8. Concentratorのパスワードを変更した管理コンソールからノードを再登録します。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

AVSソフトウェアバージョン5.1.0には、このドキュメントで説明されている脆弱性に対する修正が含まれています。

AVSソフトウェアは、cisco.comの次の場所からダウンロードできます。

- AVS 3120 5.1.0(登録ユーザ専用)
- AVS 3180 5.1.0(登録ユーザ専用)

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

この脆弱性は、シスコの社内テストで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080123-avs

改訂履歴

リビジョン 1.0	2008年1月23日	初版リリース

利用規約

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。