AVS TCPリレーの脆弱性

アドバイザリーID : cisco-sa-20060510-avs CVE-2006-2322
初公開日 : 2006-05-10 16:00
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

Cisco Application Velocity System(AVS)のデフォルト設定では、受信側TCPサービスがHTTP POSTメソッドメッセージに埋め込まれた要求を処理できる場合、到達可能な宛先TCPポートへのTCP接続の透過的なリレーが可能です。この問題はソフトウェアのアップグレードを必要とせず、該当するすべてのカスタマーのコンフィギュレーションコマンドで緩和できます。

AVSソフトウェアの修正済みバージョンは、より安全なデフォルト設定を提供するように修正されています。

シスコでは、該当するお客様が新しいAVSデバイスをインストールする際に、この脆弱性に対処するための無償ソフトウェアを提供しています。入手可能な回避策は、ソフトウェアの修正済みバージョンにアップグレードする場合でも、既存のAVSデバイスに対するこの脆弱性の影響を緩和するように手動で設定する必要があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060510-avs で公開されています。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

5.0.1より前のすべてのソフトウェアバージョンを実行しているAVS 3110および3120 Application Velocity Systemsが影響を受けます。

- AVS 3110 4.0および5.0
- AVS 3120 5.0.0

両方のデバイスの以前のすべてのバージョンと同様です。

脆弱性を含んでいないことが確認された製品

AVS 3180 Management Stationは、この脆弱性の影響を受けません。

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 3100シリーズApplication Velocity Systemは、アプリケーションパフォーマンスを向上させるエンタープライズアプライアンスです。Application Velocity Systemを使用すると、WAN全体に導入されたWebアプリケーションは、LAN環境から通常期待される応答時間を提供できます。

デフォルトでは、AVSは通常、透過プロキシとして展開されます。受信側サービスがHTTP POST方式のメッセージに埋め込まれた要求を処理できる場合、透過プロキシ機能が不正利用され、到達可能な宛先TCPポートへのTCP接続が開かれ、接続TCPポートの実際のIP送信元アドレスが隠される可能性があります。

この問題は、宛先ポート番号に基づいて接続が制限され、80および443以外のTCPポートへの接続が拒否されるようにデフォルトの動作を変更することで解決されています。

この問題は、Cisco Bug ID

- CSCsd32143(登録ユーザ専用)

注：利用可能な回避策は、ソフトウェアの修正済みバージョンにアップグレードする場合でも、既存のAVSデバイスに対するこの脆弱性の影響を緩和するように手動で設定する必要があります。

回避策

既存のAVSデバイスでは、TCP/80およびTCP/443以外のTCPポートに対するリダイレクトされたプロキシ要求の使用をブロックする設定コマンドを使用して、この問題を解決する必要があります。既存の設定の上書きを避けるために、ソフトウェアを修正バージョンにアップグレードした場合でも、このコマンドを手動で適用する必要があります。AVS Management Consoleを使用して、次の設定コマンドをfgn.confコンフィギュレーションファイルに追加する必要があります。

```
<DestinationMapping>
Name default:80 -> default:80
Name default:443 -> default:443
Name default -> localhost:9
</DestinationMapping>
```

この宛先マップでは、ポート80および443へのTCP接続だけが転送されます。AVSは、他のポート宛ての接続をリセットします。他のTCPポートへのHTTP接続を完了する必要がある場合は、上記と同じ構文を使用して構成要素に追加する必要があります。宛先がすでに構成要素に設定されている場合、

```
Name default -> localhost:9
```

設定行は、宛先マップの最後の行として追加する必要があります。宛先マップの他の行の前にこの行を追加すると、正規のトラフィックがブロックされる場合があります。宛先マップ要素を更新した後、設定変更を発行する必要があります。

AVS Management Consoleの使用方法については、http://www.cisco.com/en/US/products/ps6492/products_user_guide_chapter09186a008059be02.htmlを参照してください。

fgn.confファイルについては、http://www.cisco.com/en/US/products/ps6492/products_user_guide_chapter09186a008059bddb.html#wp1照してください。

宛先マッピングの詳細については、http://www.cisco.com/en/US/products/ps6492/products_user_guide_chapter09186a008059bddb.html#wp1照してください。

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。

この問題は、AVS 3110とAVS 3120の両方のAVSバージョン5.0.1の新規インストールで修正されています。

AVS 3110用のソフトウェアは、http://www.cisco.com/pcgi-bin/tablebuild.pl/AVS3110-5.0.1から入手できます。

AVS 3120用のソフトウェアは、http://www.cisco.com/pcgi-bin/tablebuild.pl/AVS3120-5.0.1から入手できます。

注：利用可能な回避策は、ソフトウェアの修正済みバージョンにアップグレードする場合でも、既存のAVSデバイスに対するこの脆弱性の影響を緩和するように手動で設定する必要があります。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco PSIRTは、AVSを使用して未承諾の商業目的の電子メールを送信し、メッセージの実際の発信元を隠蔽している例を認識しています。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060510-avs

改訂履歴

リビジョン 1.0	2006年5月10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。